EUSKAL HERRIKO AGINTARITZAREN ALDIZKARIA

BOLETÍN OFICIAL DEL PAÍS VASCO

Itundutako posta–ordaina: 8/98

Internet
www.euskadi.net

Franqueo concertado: 8/98

Administrazioa: Donostia kalea, 1
Legezko Gordailua: VI – 286 – 78 – VITORIA–GASTEIZ

Administración: c/ Donostia–San Sebastián, 1
Depósito Legal: VI – 286 – 78 – VITORIA–GASTEIZ

Xedapen Orokorrak

EUSKAL HERRIKO UNIBERTSITATEA

EBAZPENA, 2008ko irailaren 4koa, Euskal Herriko Unibertsitateko idazkari nagusiarena, Datu Pertsonalak Babesteari buruzko UPV/EHUren Arautegia Euskal Herriko Agintaritzaren Aldizkarian argitaratzeko agindua emateko dena.

Disposiciones Generales

UNIVERSIDAD DEL PAÍS VASCO

RESOLUCIÓN de 4 de septiembre de 2008, del Secretario General de la Universidad del País Vasco / Euskal Herriko Unibertsitatea, por la que se ordena la publicación en el Boletín Oficial del País Vasco del Reglamento de la UPV/EHU de Protección de Datos de Carácter Personal.

ERANSKINA

DATU PERTSONALAK BABESTEARI BURUZKO UPV/EHUren ARAUTEGIA

ZIOEN AZALPENA

Egunero erabiltzen dira datu pertsonalak UPV/EHUren ikastegietan, sailetan, ikerketa-institutuetan, Errektoregoan, errektoreordetzetan eta gainerako erakunde eta zerbitzuetan. Datu horiek batez ere ikasle, irakasle, ikerlari eta administrazio eta zerbitzuetako langileenak dira. Baina unibertsitateaz kanpokoak direnen datuak ere erabiltzen dira; adibidez, beste erakunde batzuetako ordezkarienak, azpikontratataturiko enpresetako langileenak eta ikerketa zientifikoetarako beren burua eskaintzen dutenenak.

Beraz, alde batetik, UPV/EHUk berarekin harremana duten pertsonei buruzko datuak behar izaten ditu; alabaina, beste alde batetik, azken urteetan indarra hartu du datu pertsonalak babesteari buruzko araudiak. Hala, datu pertsonalak isilpekoak izango badira, eta aldi berean UPV/EHUk unibertsitate publiko gisa dituen eginkizunak betetzerik izango badu, bi alderdi horien arteko oreka gordeko duten mekanismoak asmatu behar dira.

Hori dela eta, komenigarria iruditu zaigu arautegi hau onartzea; izan ere, UPV/EHUri datu pertsonalak babestearen inguruko eginbideak betetzen lagunduko dio, eta datu pertsonalak erabiltzen dituzten langileentzat erreferentea izango da.

I. TITULUA

XEDAPEN OROKORRAK

1. artikulua.– Helburua.

Arautegi honen helburua da UPV/EHUk bere esku dituen datu pertsonalen erabilera arautzea, datu pertsonalak babesteari buruzko legeak eta hura garatzeko xedapenek agintzen dutenarekin bat etorriz, datu horien jabeen ohorea eta intimitatea errespetatuz beti, eta aldi berean unibertsitateak bere eginkizunak betetzen dituela bermatuz, irakaskuntza, ikerketa eta azterlanen bidez goi mailako hezkuntza-zerbitzu publikoa eskaintzen duen erakundea den aldetik.

2. artikulua.– Aplikazio eremua.

UPV/EHUn arautegi hau aplikatuko zaie euskarri fisikoan erregistraturik eta erabilgarri dauden datu pertsonalei, eta datu horiek ondoren izan dezaketen edozein erabilera-moduri.

ANEXO

REGLAMENTO DE LA UPV/EHU PARA LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

EXPOSICIÓN DE MOTIVOS

En los Centros, Departamentos e Institutos Universitarios de Investigación de la UPV/EHU, así como en el Rectorado y Vicerrectorados, y demás entes y servicios de la Universidad, se trata diariamente con datos de carácter personal. Estos datos pertenecen principalmente al alumnado, al personal docente e investigador y al personal de administración y servicios, pero también corresponden a personas ajenas a la Universidad como representantes de otras instituciones, trabajadores y trabajadoras de empresas subcontratadas y particulares objeto de investigaciones científicas.

Tal necesidad de la UPV/EHU de valerse de datos de personas que se relacionan con la misma y, a su vez, el fortalecimiento experimentado en los últimos años por la regulación relativa a la defensa de datos de carácter personal, hacen necesario idear los mecanismos necesarios para lograr un equilibrio entre la confidencialidad de los datos de carácter personal y el hecho de que la UPV/EHU, como universidad pública, pueda llevar a cabo las funciones que le son propias.

Por todo ello, se ha considerado conveniente aprobar este Reglamento, el cual además de contribuir a que la UPV/EHU cumpla con sus obligaciones en el ámbito de la protección de datos de carácter personal, aspira a convertirse en referente para el personal de la misma que trate con datos de carácter personal.

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1.– Objeto.

En el marco del respeto de lo establecido en la legislación relativa a la protección de datos de carácter personal y sus disposiciones de desarrollo, el presente Reglamento tiene como objeto regular el tratamiento de los datos de carácter personal en manos de la UPV/EHU protegiendo, en todo caso, el honor e intimidad de las personas titulares de dichos datos y garantizando, al mismo tiempo, el cumplimiento por parte de la Universidad de las funciones que le son propias en su calidad de entidad dedicada al servicio público de la educación superior mediante la docencia, la investigación y el estudio.

Artículo 2.– Ámbito de aplicación.

Este Reglamento será de aplicación en la UPV/EHU a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de esos datos.

3. artikulua.– Legedia.

3.1.– Datu pertsonalak babesteari dagokionean UPV/EHUK errespetatu beharreko oinarrizko arautegiak honako hauek dira:

a) 95/46/EE Zuzentaraua, datu pertsonalen tratamendua eta zirkulazio askea dela-eta, pertsona fisikoak babesteari buruzkoa.

b) Espainiako konstituzioaren 18.4 artikulua.

c) Datu Pertsonalak Babesteari buruzko 15/1999 Lege Organikoa, abenduaren 13koa (aurrerantzean DBLO).

d) Abenduaren 21eko 1720/2007 Errege Dekretua, Datu Pertsonalak Babesteari buruzko abenduaren 13ko 15/1999 Lege Organikoa garatuko duen erregelamendua onartzen duena (aurrerantzean DBLOGE).

e) 2/2004 Legea, otsailaren 25ekoa, Datu Pertsonaletarako Jabetza Publikoko Fitxategiei eta Datuak Babesteko Euskal Bulegoa Sortzeari buruzkoa.

f) 308/2005 Dekretua, urriaren 18koa, datu pertsonaletarako jabetza publikoko fitxategiei eta Datuak Babesteko Euskal Bulegoa sortzeari buruzko otsailaren 25eko 2/2004 Legea garatzen duena.

3.2.– Arau horiek aldaketaren bat izanez gero, arautegi honetan indarreko xedapenen gaineko erreferentzia egiten denean, ulertuko da aldaketen ondoriozko xedapen berriari eta haren indarraldiari egiten zaion erreferentzia dela. Halaber, aldian behin arautegi hau berrikusi egingo da, izan daitezkeen arauzko eskakizun berrien arabera. Arautegiaren bertsio eguneratua unibertsitatearen web-orrian egongo da eskuragarri (www.ehu.es/babestu).

4. artikulua.– Definizioak.

4.1.– Arautegi honen arabera, jarraian zerrendatzen ditugun oinarrizko kontzeptuak, datu pertsonalak babestearen ingurukoak, honela ulertuko dira:

a) Datu pertsonalak: edozein informazio (zenbakizko informazioa, alfabetikoa, grafikoa, fotografikoa, akustikoa edo bestelakoa), identifikatutako edo identifika daitezkeen pertsona fisikoen gainekoa.

b) Pertsona identifikagarria: identitate zehazgarria duen pertsona. Identitate hori modu zuzenean nahiz zeharkakoan zehaztu daiteke, bere identitatearen hainbat alderdi (identitate fisikoa, fisiologikoa, psikikoa, ekonomikoa, kulturala edo soziala) ukitzen dituen informazioaren bidez. Pertsona fisiko bat ez dela identifikagarria ulertuko da, hura identifikatzeak neurriz kanpoko lanak ematen baditu eta denbora gehiegi eskatzen badu.

c) Bereziki babestutako datuak dira ideologiari, erlijioari, sinesmenei, sindikatu-bazkidetzari, arrazari, osasunari, bizitza sexualari edo arau-hauste penal edo administratiboei buruzkoak.

Artículo 3.– Escenario legal.

3.1.– La normativa básica que la UPV/EHU debe respetar en el ámbito de la protección de datos de carácter personal es la siguiente:

a) Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

b) Artículo 18.4 de la Constitución española.

c) Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD).

d) Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, RDLOPD).

e) Ley 2/2004, de 25 de febrero, de Ficheros de datos de Carácter Personal de Titularidad pública y de Creación de la Agencia Vasca de Protección de Datos.

f) Decreto 308/2005, de 18 de octubre, por el que se desarrolla la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos.

3.2.– En el caso de que se produzcan cambios normativos, las referencias realizadas en este Reglamento a las disposiciones vigentes a su entrada en vigor serán consideradas realizadas a las que las sustituyan. Asimismo, este Reglamento será periódicamente actualizado en función de los nuevos requisitos normativos que puedan ser exigidos. La versión actualizada del Reglamento estará disponible en la página web de la Universidad (www.ehu.es/babestu).

Artículo 4.– Definiciones.

4.1.– A la luz del presente Reglamento, se entenderán de la siguiente manera los conceptos básicos en materia de protección de datos de carácter personal indicados a continuación:

a) Datos de carácter personal: cualquier información numérica, alfabética, gráfica, fotográfica, acústica o del cualquier otro tipo concerniente a personas físicas identificadas o identificables.

b) Persona identificable: toda persona cuya identidad pueda determinarse directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionadas.

c) Datos especialmente protegidos: datos que se refieren a ideología, religión, creencias, afiliación sindical, origen racial, salud, vida sexual o infracciones penales o administrativas.

d) Osasunari buruzko datu pertsonalak: gizabanako batek izan duen, duen, edo izan dezakeen osasun fisikoari nahiz mentalari buruzko datuak. Pertsonen osasunari buruzko datutzat hartzen dira, bereziki, elbarritasun maila edo informazio genetikoa.

e) Datuen tratamendua: eragiketa eta prozedura teknikoa da -batzuetan automatizatua, beste batzuetan ez-, eta datuak bildu, gorde, grabatu, landu, aldatu, kontsultatu, erabili, blokeatu, ezabatu eta ezerezteko aukera ematen du. Komunikazio, kontsulta, elkarkonexio eta transferentzien eraginez datuak uztea ere datuak tratatzea da.

f) Fitxategia: datu pertsonalen multzo antolatua, irizpide zehatzei jarraituz datuak eskuratzeko aukera ematen duena, datu-multzoa sortu, jaso, antolatu, eta eskuratzeko modua edozein dela ere.

g) Datu-fitxategi ez-automatizatua: pertsona fisikoei buruzko datu pertsonalen multzo antolatua, ez-automatizatua, eta irizpide zehatzen arabera egituratua. Multzo horretako datu pertsonalak eskuratzeak ez du neurriz kanpoko ahaleginik eskatzen, datu horiek zentralizaturik egon ala ez, edo erabilgarritasun irizpideen nahiz geografikoen arabera banaturik ala edo ez.

h) Ukitua edo interesduna: tratatu beharreko datuen titularra den pertsona fisikoa.

i) Interesdunaren adostasuna: interesdunak bere datu pertsonalak tratatzeari emandako baiezkoa. Interesdun horrek berak hala nahita, inork inola estutu gabe, zalantzarako biderik eman gabe, berariaz eta zer egiten duen jakinda eman beharko du baiezko hori.

j) Disoziazio-prozedura: identifikatutako norbaitekin edo identifikagarria den norbaitekin lotu ezin daitekeen informazioa ematen duen datu pertsonalen tratamendua.

k) Datu disoziatua: ukitua edo interesduna identifikatzen uzten ez duen datua.

l) Datuak uztea edo jakinaraztea: interesduna ez den beste pertsona bati datuak ezagutaraztea.

m) Datu-hartzailea edo datuen lagapen-hartzailea: ezagutarazten diren datuak hartzen dituen pertsona fisikoa edo juridikoa, publikoa nahiz pribatua, edo administrazio-organoa. Halaber, datu-hartzaileak izan daitezke nortasun juridikorik gabeko erakundeak, datuen trafikoan jokatzen dutenak trafiko horretatik aparte daudenen moduan.

n) Tratamenduaren arduraduna: UPV/EHUrekin lotura juridikoa duen pertsona fisikoa edo juridikoa, aginte publikoa, zerbitzua edo beste edozein erakunde, UPV/EHUren aginduz, eta zerbitzu bat prestatzeko helburu bakarrarekin, datu pertsonalak tratatzen dituena, berak bakarrik edo beste batzuekin batera.

d) Datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

e) Tratamiento de datos: cualquier operación o procedimiento técnico, sea o no automatizado, que implique la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

f) Fichero: todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

g) Fichero no automatizado: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos de carácter personal, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

h) Afectado, afectada, interesada o interesado: persona física titular de los datos que sean objeto de tratamiento.

i) Consentimiento del interesado o interesada: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado o la interesada consienta el tratamiento de datos de carácter personal que le conciernen.

j) Procedimiento de disociación: todo tratamiento de datos de carácter personal de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

k) Dato disociado: aquel que no permite la identificación de un afectado, afectada o interesada, interesado.

l) Cesión o comunicación de datos: tratamiento de datos que supone su revelación a una persona distinta del interesado.

m) Destinatario o cesionario: la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos. Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

n) Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos de carácter personal por cuenta de la UPV/EHU, como consecuencia de la existencia de una relación jurídica que le vincula con la misma y delimita el ámbito de su actuación para la prestación de un servicio.

o) Hirugarrena: pertsona fisikoa edo juridikoa, aginte publikoa edo pribatua, edo administrazio-organoa, ez dena izango ez ukitua edo interesduna, ezta fitxategiaren barne-erantzulea [5.4.b) artikuluan zehaztua] edo tratamenduaren arduraduna ere. Halaber, ez da izango datuak tratatzeko fitxategiaren barne-erantzulearen edo tratamenduaren arduradunaren baimena jaso duen inor. Halaber, hirugarrenak izan daitezke nortasun juridikorik gabeko erakundeak, datuen trafikoan jokatzen dutenak trafiko horretatik aparte daudenen moduan.

p) Jendearen eskurako iturriak: arauek ezarritako inongo mugarik gabe, edonork kontsulta ditzakeen fitxategiak dira, eta kontsulta egin ahal izateko ez da inolako baldintzarik bete behar, kasuan kasuko ordainketaren bat egitea ez bada. Jendearen eskurako iturriak honako hauek baino ez dira izango: sustapeneko errolda; komunikazio elektronikoetarako zerbitzuen gidaliburuak, berariazko araudiak ezartzen duen moduan; eta profesionalen taldeko pertsonen zerrendak, honako datu hauek baino ez dituztenak: izena, titulua, lanbidea, jarduera, maila akademikoa, helbidea, eta taldekoa izatearen adierazpena. Era berean, jendearen eskurako iturriak dira egunkariak eta aldizkari ofizialak, eta gizarteko hedabideak.

q) Ezereztea: prozedura, zeinaren bitartez arduradunak datuak erabiltzeari uzten dion. Ezerezteak datuak blokeatzea ekarriko du; hau da, datu horiek identifikatu eta gorde egingo dira, inork erabili ez ditzan. Alabaina, administrazio publikoen, epaileen eta auzitegien esku jar daitezke, datuen tratamenduaren ondorioz sor daitezkeen erantzukizunak aintzat hartzeko, betiere erantzukizun horien preskripzio-epeak iraun bitartean. Epe hori amaitu ondoren, datuak ezabatu egin beharko dira.

r) Kentzea, ezabatzea: datu pertsonalak tratatzearen ondorioz sor daitezkeen erantzukizunen preskripzio-epea amaitu ondoren, ezereztutako datu pertsonalak fisikoki ezabatzea.

s) Erabiltzailea: datuak atzitzeko edo datuak lortzeko baliabideak erabiltzeko baimena duen pertsona edo prozesua. Erabiltzailetzat hartuko dira, erabiltzaile fisiko bat identifikatzeko beharrik izan gabe, datuak eskuratzeko edo datuak lortzeko baliabideak erabiltzeko aukera ematen duten prozesuak. «Erabiltzaileen profilak» erabiltzaile-taldeek dituzten sartzeko baimenak dira.

4.2.– Arautegi honen ondorioetarako, jarraian zerrendatzen diren kontzeptuak, hartu beharreko segurtasun-neurriekin zerikusia dutenak, honela ulertu behar dira:

a) Informazio-sistema: datu pertsonalak gorde eta erabiltzeko fitxategi, tratamendu, programa, euskarri eta ekipamenduen multzoa.

b) Tratamendu-sistema: informazio-sistema bat antolatu edo erabiltzeko modua. Tratamendu-sistemaren

o) Tercero: la persona física o jurídica, autoridad pública o privada, u órgano administrativo distinto del afectado, afectada, interesada o interesado, de la persona Responsable Interno del fichero [definido en el artículo 5.4.b.)], del Encargado o Encargada del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del Responsable Interno del fichero o del Encargado o Encargada del tratamiento. Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

p) Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencias que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, las guías de servicios de comunicaciones electrónicas en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación social.

q) Cancelación: procedimiento en virtud del cual la persona responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.

r) Supresión, borrado: la eliminación física de los datos de carácter personal cancelados una vez cumplido el plazo de prescripción de las posibles responsabilidades nacidas del tratamiento de dichos datos.

s) Usuario o Usuaria: persona o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de una usuaria o un usuario físico. Los «perfiles de usuarios» consisten en accesos autorizados a un grupo de usuarios o usuarias.

4.2.– A los efectos del presente Reglamento, los conceptos recogidos a continuación relacionados con las medidas de seguridad a adoptar serán entendidos de la siguiente manera:

a) Sistema de información: conjunto de ficheros, tratamientos, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

b) Sistema de tratamiento: modo en que se organiza o utiliza un sistema de información. Atendiendo

arabera, informazio-sistemak izan daitezke automatizatuak, ez-automatizatuak, edo erdi-automatizatuak.

c) Baliabidea: informazio-sistema baten edozein osagai.

d) Baimendutako atzipena: erabiltzaileari ematen zaion baimena, hainbat baliabide erabil ditzan.

e) Identifikazioa: erabiltzaile baten identitatea ezagutzeko prozedura.

f) Autentifikazioa: erabiltzaile baten identitatea egiaztatzeko prozedura.

g) Sarbide-kontrola: identitatea egiaztatutakoan, datuak eta baliabideak atzitzeko aukera ematen duen mekanismoa.

h) Pasahitza: isilpeko informazioa, askotan karaktere-kate batez osaturikoa, erabiltzaile baten identitatea kautotzeko edo baliabide bat atzitzeko erabil daitekeena.

i) Fitxategi iragankorra: erabiltzaile edo prozesu batek lan egiteko sortutako fitxategia, inoizka egiten den tratamendu baterako, edo tratamendu bat burutzeko bitarteko urratsa emateko.

j) Segurtasun-gorabehera: datuen segurtasunean eragiten duen edo eragin dezakeen edozein irregulartasun.

k) Euskarria: datuak eduki edo gordetzen dituen objektu fisikoa, edo informazio-sistema batean erabil litekeen objektua, datuak grabatzeko edo berreskuratzeko balio duena.

l) Segurtasun-kopia: fitxategi automatizatu bateko datuen kopia egitea, datuak berreskuratzeko moduko euskarri batean.

m) Dokumentazioa: erregistraturiko informazioa duen euskarri fisikoa (euskarri hori izan daiteke idazkia, seinalea, grafikoa, soinua, irudia, pelikula, argazkia, zinta magnetikoa, zinta mekanografikoa, kaseta, diskoa, CD-Roma, DVDa, kanpoko biltegiragailua, edo beste edozer).

n) Dokumentuen transmisioa: dokumentuetako informazioa lekualdatu, jakinarazi, bidali, eman edo zabaltzea.

5. artikulua.– Arduradunak.

5.1.– Eguneroko lanean edo noizean behin datu pertsonalak erabiltzen dituzten UPV/EHUko kide guztiek errespetatu beharko dituzte datu pertsonalen inguruko arauak. Unibertsitateko langileak zer betebehar dituzten jakiteaz arduratuko dira. Halaber, arautegi honek agintzen duena betetzen ez badute, izan ditzaketen diziplinazko ondorioak, edo hirugarrenen aurrean izan ditzaketenak, ezagutu behar dituzte.

5.2.– Beren menpeko langileak dituztenek, datu pertsonalak babestearen inguruko betebeharrak ezagutzeko prestakuntza egokia eman beharko diete haiei;

al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

c) Recurso: cualquier parte componente de un sistema de información.

d) Accesos autorizados: autorizaciones concedidas a un usuario o usuaria para la utilización de los diversos recursos.

e) Identificación: procedimiento de reconocimiento de la identidad de una usuaria o usuario.

f) Autenticación: procedimiento de comprobación de la identidad de un usuario o usuaria.

g) Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

h) Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o usuaria o en el acceso a un recurso.

i) Fichero temporal: fichero de trabajo creado por usuarios o procesos que es necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

j) Incidencia: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

k) Soporte: objeto físico que almacena o contiene datos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

l) Copia de respaldo: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

m) Documentación: todo escrito, señal, gráfico, sonido, dibujo, película, fotografía, cinta magnética, cinta mecanográfica, cassette, disco, CD-Rom, DVD, dispositivos externos de almacenamiento u otro medio físico en el que se haya registrado información.

n) Transmisión de documentos: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

Artículo 5.– Responsables.

5.1.– Todo el personal de la UPV/EHU que realice tratamientos de datos de carácter personal, de forma general o excepcional, deberá respetar la normativa al respecto. Los trabajadores y trabajadoras de la Universidad deberán preocuparse por conocer sus obligaciones y ser conscientes de las consecuencias, de carácter disciplinario o ante terceros, en el caso de actuar al margen de lo establecido en este Reglamento.

5.2.– Quienes tengan personal a su cargo, deberán formarlo debidamente en sus deberes en relación con la protección de datos de carácter personal, prestando es-

arreta berezia jarriko dute beren taldeetan sartzen diren langile berriengan.

5.3.– Datu pertsonalak babesteari buruzko arauek agintzen dutenaren itzalpean, UPV/EHUk bere gain hartzen du ardura korporatiboa, unibertsitatean datu pertsonalak eraginkortasunez eta egokitasunez babesteko duen eginbeharra betetzen duela bermatzeko. Beraz, UPV/EHUk bertako langileei informazioa eta prestakuntza emateko ekintzak antolatuko ditu aldian behin, batez ere datu pertsonal ugari eta bereziki babestutako datuak erabiltzen dituztenentzat.

5.4.– UPV/EHUk datu pertsonalak babesteari buruzko arautegia egiazki ezartzeari dagokionez, errektorea izango ezarpen horren arduradun nagusia, eta unibertsitateak aitorturiko fitxategi guztien azken arduraduna ere bai. Era berean, datu pertsonalak babesteari dagokionez, UPV/EHUk honako arduradun hauek izango ditu:

a) DBLO segurtasun-arduraduna: UPV/EHUko informazioaren segurtasuna zaintzeko estrategia orokorra zehazteaz gain, estrategia hori bete egiten dela eta datu pertsonalak babesteari buruzko arauek agindutakora egokitzen dela egiaztatzeko ardura duen pertsona. Bere eginkizunetako bat da datuak atzitzeko, zuzentzeko, ezerezteko eta datuen aurka egiteko eskubideak baliatu ahal izateko aukez daitezkeen eskaerak bideratzea, baita adostasuna baliogabetzekoak eta balorazioak aurkaratzekoak ere.

b) Fitxategiaren barne-erantzulea: esleitzen zaizkion fitxategiak zertarako izango diren, zer eduki izango duten eta nola erabiliko diren erabaki ahal izateko errektorearen eskuordetzea jaso duen pertsona. Fitxategiaren barne-erantzuleak datu pertsonalak babesteari buruzko arautegiak esleitzen dizkion eginkizunez gain, arautegi honek «fitxategiaren edo tratamenduaren erantzulea» den pertsonari esleitzen dizkionak beteko ditu.

c) Segurtasun Informatikorako eta Dokumentuen Gestiorako Batzordea: «Segurtasun-arduraduna» izenekoaren eginkizuna (DBLOGEk zehaztutakoa) betetzen duen organoa. Eginkizun hori UPV/EHUko fitxategi guztietan aplika daitezkeen segurtasunerako neurrien ezarpena koordinatu eta kontrolatzean datza.

d) Datuak Babesteko Batzordea: Arautegi hau benetan ezartzeko koordinazio- eta kontrol-lanez arduratzen dena; eta, datuak babesteari dagokionez, UPV/EHUren jarduera-ildo nagusiak ezartzeko ardura duena.

e) Errektorego, errektoreordetza, ikastegi, sail, unibertsitateko ikerketa-institutu, unibertsitateko zerbitzu edo beste organo batzuetako datu pertsonalen babeserako koordinatzailea: Errektorego, errektoreordetza, ikastegi, sail, unibertsitateko ikerketa-institutu, unibertsitateko zerbitzu edo bestelako organoen arduradun nagusiek bere gain hartuko dute erantzukizuna, unibertsitateko datu pertsonalak babesteari buruzko arautegia

pecial atención a las nuevas personas que se incorporen a sus equipos.

5.3.– La UPV/EHU asume su responsabilidad corporativa en relación con el deber de garantizar una protección de datos de carácter personal eficaz y válida en el ámbito de la Universidad en el marco de lo establecido en la normativa relativa a la protección de datos de carácter personal. En consecuencia, la UPV/EHU planificará periódicamente acciones informativas y formativas dirigidas a su personal, y de una manera preferente a quienes traten con más datos de carácter personal o datos especialmente protegidos.

5.4.– El Rector o Rectora será el máximo o la máxima responsable de la efectiva aplicación de la normativa en materia de protección de datos de carácter personal por parte de la UPV/EHU, y Responsable último de todos los ficheros declarados por la Universidad. Asimismo, en la UPV/EHU se identifican las siguientes figuras con responsabilidad en la protección de datos de carácter personal:

a) Responsable de Seguridad LOPD: persona encargada de definir y velar por el cumplimiento de la estrategia global en materia de seguridad de la información de la UPV/EHU y, especialmente, la correcta adecuación de la misma a lo establecido en la normativa relativa a la protección de datos de carácter personal. Entre sus funciones estará la de canalizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, las revocaciones de consentimiento y las impugnaciones de valoraciones que puedan presentarse.

b) Responsable Interno de fichero: persona que, por delegación del Rector o Rectora, decide sobre la finalidad, contenido y el tratamiento del o de los ficheros que le sean asignados. La persona Responsable Interno del fichero cumplirá con las funciones asignadas por la normativa en materia de protección de datos de carácter personal y el presente Reglamento a la persona «Responsable del fichero o tratamiento».

c) Comité de Seguridad Informática y Gestión Documental: órgano que realiza la función de «Responsable de Seguridad» (según definición del RDLOPD) de todos los ficheros de la UPV/EHU, y cuya función consiste en coordinar y controlar las medidas de seguridad aplicables a los citados ficheros.

d) Comisión para la Protección de Datos: órgano encargado de llevar a cabo la coordinación y control de la efectiva implantación del presente Reglamento y establecer las pautas generales de actuación de la UPV/EHU en cuestión de protección de datos.

e) Coordinador o Coordinadora de la protección de datos de carácter personal de Rectorado, Vicerrectorado, Centro, Departamento, Instituto Universitario de Investigación, servicio u otro organismo universitario: el máximo o la máxima persona responsable del Rectorado, Vicerrectorado, Centro, Departamento, Instituto Universitario de Investigación, servicio u organismo universitario asumirá la responsabilidad de difundir,

zabaldu, ezarri eta benetan betetzen dela bermatzeko, bakoitzak dagokion arloan, eta unibertsitateko datu pertsonalak babesteko gainerako erantzuleekin koordinatuz eta lankidetzan arituz; era berean, lan horiek egiteko beste pertsona batzuk izenda ditzakete, baina beren erantzukizuna horien gain utzi gabe.

5.5.– Arautegi honetako IV. Tituluan zehazten dira datu pertsonalak babesteko unibertsitateko arduradun horien eginkizunak.

II. TITULUA

DATU PERTSONALEN TRATAMENDUA

1. KAPITULUA
DATU PERTSONALEN BILKETA

6. artikulua.– Datuak bildu eta tratatzeko modua.

6.1.– Datu pertsonalak zintzotasunez eta legea betez tratatuko dira; beraz, debekatuta dago datuak biltzeko iruzurra egitea, edo legezkoak ez diren bide makurrak erabiltzea.

6.2.– Helburu zehatz, esplizitu eta legezkok betetzeko baino ez dira bilduko datu pertsonalak.

6.3.– UPV/EHUk uneoro aintzat hartuko du datu pertsonalak haien jabeenak baino ez direla dioen printzipioa, eta ez ditu ez eskatuko ez tratatuko, helburu zehatzetarako ez bada, eta horretarako behar bezalako eskubiderik ez badu.

7. artikulua.– Erabilera eta helburuari buruzko informazioa.

7.1.– Datuak biltzen dituzten formularioek, paperean nahiz monitorean daudenek, berariaz informazio hau eman beharko dute, zehatz eta argi:

a) Datu pertsonalak tratatzeko fitxategi bat dagoela adierazi beharko dute, datuak zertarako biltzen diren jakinarazi, eta informazio hori norentzat izango den esan.

b) Lagapen-hartzaileak zeintzuk diren edo zer kategoria duten adierazi beharko dute, horien jarduera zehatza eta esplizitua, behintzat, zein den adieraziz.

c) Egiten diren galderak erantzutea derrigorra edo aukerakoa den argitu beharko dute.

d) Datuak emateak edota ez emateak dituen ondorioak azaldu beharko dituzte.

e) Datuak atzitzeko, zuzentzeko, ezerezteko eta datuen aurka egiteko eskubideak daudela adierazi beharko dute, eta eskubide horiek zein organoren aurrean balia daitezkeen jakinarazi.

implantar y garantizar la efectiva aplicación de la normativa relativa a la protección de datos de carácter personal de la Universidad en el ámbito que le corresponda, en coordinación y colaboración con el resto de responsables en materia de protección de datos de carácter personal de la Universidad, y pudiendo designar a su vez a otras personas para estar tareas sin que ello implique una delegación de su responsabilidad.

5.5.– En el Título IV del presente Reglamento se concretan las previsiones respecto a los responsables universitarios en materia de protección de datos.

TÍTULO II

TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

CAPÍTULO 1
RECOGIDA DE DATOS DE CARÁCTER PERSONAL

Artículo 6.– Modo de recabar y tratar los datos.

6.1.– Los datos de carácter personal deberán ser tratados de forma leal y lícita, por lo que se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

6.2.– Los datos de carácter personal sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas.

6.3.– La UPV/EHU tendrá presente, en todo momento, el principio de que los datos de carácter personal son propiedad de las personas a las que se refieren y no los solicitará ni hará uso de ellos salvo para aquellas finalidades para las que esté facultada debidamente.

Artículo 7.– Información sobre el uso y la finalidad.

7.1.– Los formularios de recogida de datos, tanto en papel como en pantalla, deberán incluir de modo expreso, preciso e inequívoco la siguiente información:

a) la existencia de un fichero o tratamiento de datos de carácter personal, la finalidad de la recogida de éste y los destinatarios de la información;

b) en su caso, los cesionarios o categorías de cesionarios de los datos, delimitados al menos por el tipo de actividad, determinada y explícita, a la que los mismos se dediquen;

c) el carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas;

d) las consecuencias de la obtención de los datos o de la negativa a suministrarlos;

e) la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, y del órgano ante el que se ejercitan tales derechos.

f) Fitxategiaren edo tratamenduaren pertsona erantzulearen identitatea eta helbidea adierazi beharko dituzte.

7.2.– Eskatutako datu pertsonalak nolakoak diren edo zer egoeratan biltzen diren ikusita c) eta d) atalei dagokien informazioa ondorioztatzerik baldin badago, atal horiek ez dira derrigorrak izango.

7.3.– Informaziorako eskubideari ahalik eta indar gehien emateko, unibertsitateak, formularioen bidez datu pertsonalak biltzen dituenean, arautegi hau interneten eskura daitekeela adieraziko du, bai bere web-orrian, bai Datuak Babesteko Euskal Bulegoaren orrian.

7.4.– Datu pertsonalak interesdunaren bitartez jasotzen ez dituenean, UPV/EHUk, datu horiek erregistratzen dituen egunetik kontatzen hasi eta hiru hilabeteko epean, berariaz honako informazio hau eman beharko dio interesdunari, modu zehatz eta argian, baldin eta lehenago halako jakinarazpenik egin ez badio:

a) tratamenduaren edukia;

b) datuen jatorria;

c) datuak atzitzeko, zuzentzeko, ezerezteko eta datuen aurka egiteko eskubidea baliatzeko aukera.

d) fitxategiaren edo tratamenduaren erantzulearen identitatea eta helbidea.

7.5.– Arautegi honetako I.I.E. eranskinean hirugarrenei buruzko datuak biltzen dituzten formularioetan sartu behar den informazio-klausula dago jasota. Informazio-klausula horren edukia izan daitekeen txikiena da; beraz, zenbaitetan beharrezkoa izango da eduki hori beste zerbaitekin osatzea; adibidez, unibertsitateak etorkizunean datuak uzteko eskubidea izateko baimeneskaera egiteko formularekin.

8. artikulua.– Datuen kalitatea.

8.1.– Datu pertsonalak bildu eta tratatzerako, kontuan hartu beharko da zertarako jaso nahi diren, eta ezinbestekoa izango da datu horiek egokiak izatea helburu zehatz, argi eta legezko horretarako; halaber, datuek ez dute neurriz gainekoak izan beharko.

8.2.– Tratatuko diren datu pertsonalak ez dira erabiliko datu horiek biltzearen helburuarekin bat ez datorren xedeetarako.

8.3.– Datu pertsonalak zehatzak eta eguneratuak izango dira; beraz, beren jabearen uneko egiazko egoera adieraziko dute. Datuak zuzenean euren jabearen eskutik biltzen badira, hark emandako datuak hartuko dira egiazkotzat. Erregistratutako datu pertsonal guztiak edo horietako batzuk okerrak badira, edo osatu gabe badaude, okerra ezagutzen den egunetik kontatzen hasita hamar eguneko epea egongo da akats horiek zuzentzeko edo datuak ezerezteko, kalterik egin gabe arautegi ho-

f) la identidad y dirección de la persona Responsable del fichero o tratamiento.

7.2.– No será necesaria la inclusión del contenido de los apartados c) y d) anteriores, en el caso de que dicha información pueda deducirse de la naturaleza de los datos de carácter personal que se solicitan o de las circunstancias en que se recaban.

7.3.– Con el fin de llevar el derecho de información a su máxima expresión, la Universidad informará de la existencia del presente Reglamento cuando recoja datos de carácter personal a través de formularios, indicando su ubicación en Internet en la web de la Universidad y en el de la Agencia Vasca de Protección de Datos para su consulta.

7.4.– Cuando los datos de carácter personal no hayan sido recabados de la interesada o interesado, éste deberá ser informado por la UPV/EHU, dentro de los tres meses siguientes al momento de registro de los datos, de forma expresa, precisa e inequívoca, salvo que ya hubiera sido informado con anterioridad, sobre:

a) el contenido del tratamiento;

b) la procedencia de los datos;

c) la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y

d) la identidad y dirección de la persona «Responsable de fichero o tratamiento».

7.5.– En el anexo I.M.I del presente Reglamento se recoge la cláusula informativa a introducir en los formularios donde se recaben datos de terceros. Se advierte que el contenido de la cláusula informativa es de carácter mínimo y, por lo tanto, en algunos casos será necesario completarla con otra serie de cuestiones como fórmulas de solicitud de autorización para futuras cesiones de datos por parte de la Universidad.

Artículo 8.– Calidad de los datos.

8.1.– Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

8.2.– Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

8.3.– Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán rectificados o cancelados en el plazo de diez días desde que se tuviese conocimiento de la inexactitud, sin perjuicio del ejercicio de

netako 14, 15, 16 eta 17. artikuluetan aitortzen diren eskubideak baliatzeko interesdunak duen aukerari.

Datu horiek lehenagotik jakinarazi badira, fitxategiaren edo tratamenduaren pertsona erantzuleak egindako zuzenketa edo ezereztea jakinarazi beharko dio lagapen-hartzaileari hamar eguneko epean. Datuak erabiltzen dituen lagapen-hartzaileak jakinarazi zaion zuzenketa edo ezereztea egin beharko du hamar eguneko epean, jakinarazpen hori jasotzen duen egunetik kontatzen hasita. Datu pertsonalen eguneratze hori ez zaio interesdunari jakinaraziko.

9. artikulua.– Helburu estatistiko, historiko edo zientifikoak dituen tratamendua.

9.1.– Datu pertsonalak helburu historiko, estatistiko edo zientifikoetarako erabiltzea ez da bateraezina izango arautegi honetako 8.2 artikuluak agintzen duenarekin. Aurreko paragrafoan aipatutako helburu horiek zehazteko, aintzat hartuko da kasu bakoitzean ezar daitekeen legea, eta bereziki honako hauek agintzen dutena: ekainaren 25eko 16/1985 Legea, Espainiako Historia Ondareari buruzkoa; maiatzaren 9ko 12/1989 Legea, Funtzio Estatistikoari buruzkoa; Ikerketa Zientifikoa Sustatu eta Koordinatzeko apirilaren 14ko 13/1986 Legea; lege horiek garatzeko xedapenak; eta gai horien inguruko autonomia erkidegoko araudia.

9.2.– DBLOGEren IX. Tituluko VII. Kapituluaren bigarren atalean ezarritako prozedurarekin bat etorriz, eta fitxategiaren edo tratamenduaren pertsona erantzuleak aurretiaz hala eskatzen badio, Datuak Babesteko Euskal Bulegoak zenbait datu osorik gordetzea erabaki dezake, goiko zatian aipatutako arauen arabera datu horiek balio historikoa, estatistikoa edo zientifikoa badute.

10. artikulua.– Datuak gordetzea eta ezereztea.

10.1.– Datuak ezereztu eta ondoren kendu edo ezabatzen ez diren bitartean, datu pertsonalak tratatuko dira datuak atzitzeko eskubidea baliatzeko aukera emanez.

10.2.– Datu pertsonalak ezereztu egingo dira, datu horien bilketa edo erregistroak zuen helbururako beharrezkoak edo egokiak izateari uzten diotenean. Alabaina, harreman edo betebehar juridiko baten ondorioz edo kontratu bat egitearen ondorioz erantzukizunen bat eskatu behar denean, datu horiek denbora batez gorde ahalko dira.

10.3.– Ezerezteak datuak blokeatzea ekarriko du; hau da, datu horiek identifikatu eta gorde egingo dira, inork erabili ez ditzan. Alabaina, administrazio publikoen, epaileen eta auzitegien esku jar daitezke, datuen tratamenduaren ondorioz sor daitezkeen erantzukizunak aintzat hartzeko, betiere erantzukizun horien preslos derechos por parte de las interesadas o los interesados reconocidos en los artículos 14, 15, 16 y 17 del presente Reglamento.

Cuando los datos hubieran sido comunicados previamente, la persona Responsable del fichero o tratamiento deberá notificar al cesionario o cesionaria, en el plazo de diez días, la rectificación o cancelación efectuada. En el plazo de diez días desde la recepción de la notificación, la cesionaria o el cesionario que mantuviera el tratamiento de los datos, deberá proceder a la rectificación o cancelación notificada. Esta actualización de los datos de carácter personal no requerirá comunicación alguna al interesado.

Artículo 9.– Tratamiento con fines estadísticos, históricos o científicos.

9.1.– No se considerará incompatible, a los efectos previstos en el artículo 8.2 del presente Reglamento, el tratamiento de los datos de carácter personal con fines históricos, estadísticos o científicos. Para la determinación de los fines a los que se refiere el párrafo anterior se estará a la legislación que en cada caso resulte aplicable y, en particular, a lo dispuesto en la Ley 12/1989, de 9 de mayo, reguladora de la Función Estadística Pública, la Ley 16/1985, de 25 junio, del Patrimonio Histórico Español y la Ley 13/1986, de 14 de abril, de Fomento y Coordinación General de la Investigación Científica y Técnica, y sus respectivas disposiciones de desarrollo, así como a la normativa autonómica en estas materias.

9.2.– La Agencia Vasca de Protección de Datos podrá, previa solicitud de la persona Responsable del fichero o tratamiento y conforme al procedimiento establecido en la Sección Segunda del Capítulo VII del Título IX del RDLOPD, acordar el mantenimiento íntegro de determinados datos, atendidos sus valores históricos, estadísticos o científicos de acuerdo con las normas a las que se refiere el apartado anterior.

Artículo 10.– Conservación y cancelación de los datos.

10.1.– Los datos de carácter personal serán tratados de forma que permitan el ejercicio del derecho de acceso, en tanto no proceda su cancelación y posterior supresión o borrado.

10.2.– Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato.

10.3.– La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales para la atención de las posibles responsabilidades nacidas del tratamiento y sólo

kripzio-epeak iraun bitartean. Epe hori amaitu ondoren, datuak kendu edo ezabatu egin beharko dira.

10.4.– Datuak kendu edo ezabatzeak esan nahi du ezereztutako datu pertsonalak fisikoki ezabatuko direla, datu pertsonalak tratatzearen ondorioz sor daitezkeen erantzukizunen preskripzio-epea amaitu ondoren.

10.5.– Edozein modutan, dokumentu eta euskarrietako datuak gorde eta ezabatzeari buruz UPV/EHUk ezartzen duena errespetatu beharko da.

11. artikulua.– Interesdunaren adostasuna.

11.1.– Legeak besterik adierazi ezean, interesdunaren adostasun garbia beharko da datu pertsonalak tratatu ahal izateko. Adostasun hori lortuko da arautegi honetako 12. artikuluan adierazitako moduren batean.

11.2.– Alabaina, honako kasu hauetan unibertsitatea ez da derrigorturik egongo erabili nahi dituen datu pertsonalen jabeei adostasuna eskatzera:

a) Unibertsitateak bere eskumenen barruan dagozkion eginkizunak betetzeko biltzen dituenean datu pertsonalak.

b) Kontratuetako, aurrekontratuetako, edo negozio-, lan- eta administrazio-harremanetako aldeei buruzko datu pertsonalak direnean, eta kontratu edo harreman horiei eusteko edo horiek betetzeko beharrezkoak direnean.

c) DBLOren 7.6 artikuluan ezarritakoaren arabera, datu pertsonalak interesdunaren bizitza edo osasuna babesteko helburuarekin erabiltzen direnean.

d) Datuak jendearen eskurako iturrietan daudenean, eta UPV/EHUk edo datu- jakinarazpena jaso duen hirugarren batek datu horiek bere legezko interesak betetzeko behar dituenean, betiere interesdunaren oinarrizko eskubideak urratzen ez badira.

11.3.– Interes orokorren bat tarteko, lege batek agintzen duenean baino ezingo dira bildu, tratatu edo utzi osasunari, bizitza sexualari edo arrazari buruzko datu pertsonalak; edo, bestela, interesdunak berariaz horretarako adostasuna agertzen duenean. Langileen osasunarekin harreman zuzena duten UPV/EHUko profesionalek haiengana jotzen duten pertsonen osasunari buruzko datu pertsonalak tratatu ahalko dituzte, osasunari buruzko eta lan-arriskuen prebentzioari buruzko indarreko araudiak ezartzen duenarekin bat etorriz.

11.4.– Ideologia, erlijio, sinesmen eta sindikatu-bazkidetzari buruzko datuak erabili ahal izateko, interesdunak idatziz agertu beharko du berariazko adostasuna. Ideologia, erlijio, sinesmen eta sindikatu-bazkidetzari

durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión o borrado de los datos.

10.4.– La supresión o borrado supone la eliminación física de los datos de carácter personal cancelados una vez cumplido el plazo de prescripción de las posibles responsabilidades nacidas del tratamiento de dichos datos.

10.5.– En todo caso, habrá que respetar lo establecido por la UPV/EHU en relación con la conservación y supresión de los datos en documentos y soportes.

Artículo 11.– Consentimiento de la persona.

11.1.– Salvo que la ley disponga otra cosa, el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado. La obtención de dicho consentimiento se realizará siguiendo alguna de las fórmulas indicadas en el artículo 12 del presente Reglamento.

11.2.– No obstante, la Universidad no tendrá la obligación de solicitar su consentimiento a las personas titulares de los datos de carácter personal de los que quiera valerse cuando desee utilizarlos en alguno de los siguientes supuestos:

a) los datos de carácter personal se recogen para el ejercicio de las funciones propias de la Universidad en el ámbito de sus competencias;

b) los datos de carácter personal se refieren a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y son necesarios para su mantenimiento o cumplimiento;

c) el tratamiento de los datos de carácter personal tiene por finalidad proteger un interés vital del interesado en los términos del artículo 7.6 de la LOPD;

d) los datos figuran en fuentes accesibles al público y su tratamiento es necesario para la satisfacción del interés legítimo perseguido por la UPV/EHU o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado o interesada.

11.3.– Respecto a los datos de carácter personal relativos a la salud, vida sexual u origen racial, estos sólo podrán ser recabados, tratados y cedidos cuando por razones de interés general así lo disponga una ley o el interesado o la interesada consienta expresamente. Las y los profesionales de la UPV/EHU directamente relacionados con la salud de los trabajadores podrán tratar los datos de carácter personal relativos a la salud de las personas que a ellos acudan, de acuerdo con lo dispuesto en la normativa vigente en materia de sanidad y de protección de la salud y prevención de riesgos laborales.

11.4.– El tratamiento de datos relativos a ideología, religión, creencias y afiliación sindical, requiere el consentimiento expreso y por escrito del interesado o interesada. En el caso de que se recabasen datos relativos a

buruzko datuak biltzen badira, interesdunari datu horiek erabiltzeko debekua ezar dezakeela jakinaraziko zaio.

11.5.– Adostasuna agertu ondoren, adostasun hori ezeztatu ahalko da, horretarako arrazoi justifikaturik egonez gero, eta atzeraeraginezko ondoriorik ez badago. Adostasuna ezeztatzeko eskaera idatziz egin beharko zaio DBLO segurtasun-arduradunari, eta horrek, dagokion fitxategiaren edo tratamenduaren pertsona erantzuleari kontsulta egin ondoren, hamar eguneko epea izango du, eskaera jasotzen duen egunetik kontatzen hasita, horri erantzun eta adostasuna ezeztatzeko. Lehenagotik jakinarazita edo utzita dauden datuak tratatzeko adostasuna ezeztatu bada, UPV/EHUk datuen jakinarazpena jaso zuenari ezeztatze horren berri eman beharko dio, baldin eta hark datuak tratatzen jarraitzen badu. I.II.E. eranskinean jasotzen da adostasuna ezeztatzeko eredua. Halaber, arautegi honetako 16. artikuluan adierazten den ezerezteko eskubidearen bitartez ere ezeztatu ahalko da adostasuna.

12. artikulua.– Adostasuna jasotzeko ereduak.

12.1.– Arautegi honetako I.III.E eranskinean dago datuak erabiltzeko berariazko baimena emateko eredua.

12.2.– Halaber, zenbait kasutan, interesdunari beste aukera batzuk emango zaizkio bere datuak tratatu edo uzteko baimena berariaz ukatu ahal izan dezan. Adibidez, fitxategiaren edo tratamenduaren pertsona erantzuleak kontratu bat egiteko prozesuaren barruan adostu nahi den kontratu-harremana mantendu, garatu edo kontrolatzeko beharrezkoak ez diren datuak tratatu edo uzteko eskaera egiten badu, interesdunak eskaerari uko egin ahalko dio, kontratua egiteko ematen zaion dokumentuan argi ikusteko moduan agertuko den lauki zuri bat markatuz, edo antzeko beste prozedura bat erabiliz.

12.3.– Legearen aginduz berariazko baimena nahitaezkoa ez denean, fitxategiaren edo tratamenduaren pertsona erantzuleak DBLOren 5. artikuluan eta DBLOGEren 12.2 artikuluan adierazitako moduan jakinarazpena egingo dio interesdunari; 30 eguneko epea emango dio datuak erabiltzeko baimena ukatu dezan, eta jakinaraziko dio datu pertsonalak erabiltzeko baimena emandakotzat hartuko dela, interesdunak epe horretan bestelakorik adierazten ez badu. Edonola ere, fitxategiaren edo tratamenduaren pertsona erantzuleak jakin egin beharko du, arrazoiren bat tarteko, jakinarazpen-itzultzerik izan den ala ez; halakorik egon bada, ezingo ditu interesdunari dagozkion datuak erabili.

la ideología, religión o creencias de la interesada o del interesado, éste será advertido de su derecho a no consentir el tratamiento de tales datos.

11.5.– Una vez dado el consentimiento, éste podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos. La revocación del consentimiento podrá realizarse mediante escrito dirigido a la persona «Responsable de Seguridad LOPD» manifestando tal decisión y éste, tras haber consultado al correspondiente Responsable de fichero o tratamiento, deberá responder expresamente en el plazo de diez días desde la recepción de la solicitud de revocación del consentimiento, materializando, en su caso, tal revocación dentro del mismo plazo. Si los datos para cuyo tratamiento se revoca el consentimiento hubieran sido comunicados previamente, la UPV/EHU deberá notificar la revocación del consentimiento efectuada a quien se hayan comunicado en el caso de que se mantenga el tratamiento por este último. El modelo de revocación del consentimiento se recoge en el anexo I.M.II. También es posible revocar el consentimiento ejerciendo el derecho de cancelación previsto en el artículo 16 del presente Reglamento.

Artículo 12.– Fórmulas para recabar el consentimiento.

12.1.– La fórmula de autorización expresa para el tratamiento de datos figura como anexo I.M.III del presente Reglamento.

12.2.– Asimismo, en determinados supuestos como por ejemplo en el caso de que la persona Responsable del fichero o tratamiento solicite el consentimiento del afectado o afectada durante el proceso de formación de un contrato para finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación contractual que se pretende acordar, se podrá permitir a la afectada o afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos posibilitándole la marcación de una casilla claramente visible y que no se encuentre ya marcada en el documento que se le entregue para la celebración del contrato o se establezca un procedimiento equivalente que le permita manifestar su negativa al tratamiento.

12.3.– En aquellos supuestos en los que el consentimiento expreso no sea exigido de manera imperativa por una ley, la persona Responsable del fichero o tratamiento podrá dirigirse al afectado, informándole en los términos previstos en los artículos 5 de la LOPD y 12.2 del RDLOPD, y deberá concederle un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal. En todo caso, será necesario que la persona Responsable del fichero o tratamiento pueda conocer si la comunicación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado o interesada.

Interesdunari bide erraza eta doanekoa eskainiko zaio, datuak tratatzeari ezetza eman diezaion. Datuak tratatzeari ezetza emateko, arautegi honi lotuko zaio bereziki posta elektronikoa erabiltzea; edo, bestela, posta-bidalketa egitea frankeo ordaindua duen gutunazalean (aurretiaz unibertsitateak emanikoa), edo beste moduren batean.

Interesdunaren adostasuna azken prozedura horri jarraituz eskatzen denean, eskaera hori egiten den egunetik kontatzen hasi eta urtebeteko epean ezingo da eskaera bera egin, datuen tratamendu eta helburuak aldatu ez badira.

2. KAPITULUA
INTERESDUNEN ESKUBIDEAK

13. artikulua.– Datuak atzitu, zuzendu, ezereztu eta datuen aurka egiteko eskubideak.

13.1.– Datuak atzitu, zuzendu, ezereztu eta datuen aurka egiteko eskubideak oso pertsonalak dira, eta interesdunak baino ezingo ditu erabili. Eskubide horiek erabiltzeko:

a) Interesdunak bere identitatea egiaztatu beharko du.

b) Interesdunaren legezko ordezkariak jokatu beharko du haren izenean, interesduna ezintasun-egoeran dagoenean edo adin txikikoa denean eta eskubide horiek bere kabuz baliatu ezin dituenean. Horretarako, egiaztatu egin beharko du legezko ordezkaria dela.

c) Berariaz borondatezko ordezkaria izendatu ahalko da eskubide horiez baliatzeko. Kasu horretan, ordeztuaren identitatea egiaztatu beharko da haren Nortasun Agiri Nazionala edo horren baliokidea den agiriren bat aurkeztuz. Halaber, egiaztatu egin beharko da interesdunak emandako ordezkaritza, egiaztatzen dena modu fidagarrian jasota uzten duen eta zuzenbidean baliozkoa den bitartekoren bat erabiliz (adibidez, notario-ahalordea), edo interesduna bera agertuz ordezkaritza hori jakinarazteko.

13.2.– Interesdunak nahitaez egiaztatu beharko du bere identitatea. Horregatik, eskubide horiek baliatzeko eskaera egitean erabiltzen diren bideek interesdunaren identitatea egiaztatzeko aukerarik ematen ez badute, ez dira aintzat hartuko eskaera horiek (adibidez, telefonoz egiten direnak).

13.3.– Gurasoek, tutoreek edo beste hirugarren batzuek ezingo dute eskuratu beren seme-alaba edo hurbilekoek UPV/EHUn duten espediente akademikoa, artikulu honetan berariaz onartzen diren kasuetan ez bada.

Datu pertsonalen titularra hiltzen denean ere ezingo dira bere datuak eskuratu. Alabaina, hildakoarekin

Deberá facilitarse a la interesada o interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos. En particular, se considerarán ajustados al presente Reglamento el que tal negativa pueda efectuarse mediante correo electrónico o su envío en sobre previamente facilitado por la Universidad con el franqueo pagado u otra modalidad postal.

Cuando se solicite el consentimiento del interesado o de la interesada a través de este último procedimiento, no será posible solicitarlo nuevamente respecto de los mismos tratamientos y para las mismas finalidades en el plazo de un año a contar de la fecha de la anterior solicitud.

CAPÍTULO 2
DERECHOS DE LOS INTERESADOS E INTERESADAS

Artículo 13.– Solicitudes de acceso, rectificación, cancelación y oposición.

13.1.– Los derechos de acceso, rectificación, cancelación y oposición son personalísimos, y serán ejercidos por la interesada o interesado. Tales derechos se ejercitarán:

a) Por el afectado o afectada, acreditando su identidad.

b) Cuando la afectada o afectado se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de estos derechos, podrán ejercitarse por su representante legal, en cuyo caso será necesario que acredite tal condición.

c) Los derechos también podrán ejercitarse a través de representante voluntario, expresamente designado para el ejercicio del derecho. En ese caso, deberá constar claramente acreditada la identidad de la persona representada mediante la aportación de copia de su Documento Nacional de Identidad o documento equivalente, y la representación conferida por aquélla por cualquier medio válido en derecho que deje constancia fidedigna (por ejemplo, poder notarial) o mediante declaración en comparecencia personal del interesado o interesada.

13.2.– Será imprescindible que la interesada o interesado acredite su identidad. Por esta razón, no serán atendidas las solicitudes de ejercicio de estos derechos que se efectúen por teléfono o cualquier otro medio que no permita acreditar la identidad de la interesada o interesado.

13.3.– Los padres, madres, tutores o cualquier otro tercero, no tendrán acceso al expediente académico o a cualquier otro dato personal de sus hijos, hijas o personas queridas vinculadas con la UPV/EHU, salvo en los supuestos expresamente aceptados por el presente artículo.

Esta imposibilidad se extiende a los datos de carácter personal de la persona fallecida. No obstante, las

lotuta dutenek, bai familia lotura bai izatezkoa, DBLO segurtasun-arduradunarengana jo dezakete hari heriotzaren berri emateko, horretarako agiri egokiak aurkeztuz eta datuak ezerezteko eskatuz, hori egiterik balego. DBLO segurtasun-arduradunak eman zaion informazioa jakinaraziko dio ukitutako fitxategiaren edo tratamenduaren pertsona erantzuleari.

13.4.– Datuak atzitzeko, zuzentzeko, ezerezteko eta datuen aurka egiteko eskubidea baliatzeko, DBLO segurtasun-arduradunari edo fitxategiaren erantzuleari idazki bat aurkeztu beharko zaio unibertsitateko erregistro orokorrean edo UPV/EHUko 2007ko maiatzaren 28ko erabakian zerrendatutako bulegoetan (2007ko abuztuaren 3ko EHAA, 149. zk.); bestela, Herri Administrazioen Araubide Juridikoaren eta Administrazio Prozedura Erkidearen azaroaren 26ko 30/1992 Legeko 38.4. artikuluak ezarritako bideak erabiliz ere aurkez daiteke idazkia. DBLO segurtasun-arduradunak jaso dituen eskaerak helaraziko dizkie ukitutako fitxategien edo tratamenduen pertsona erantzuleei. Eskaerak egiteko idazkian honako hauek agertu beharko dute:

a) Interesdunaren izen-abizenak; nortasun agiri nazionalaren kopia, edo pasaportea, edo identifikatuko duen baliozko beste dokumentu edo tresna elektronikoren bat. Interesdunaren ordezkoak identifikazio-dokumentuaz gain ordezkaritza egiaztatuko duen agiria edo tresna elektronikoa aurkeztu beharko du. Ez da NAN edo horren ordezko dokumentu baliokidearen kopiarik aurkeztu beharrik izango, identifikatzeko firma elektronikoa erabiltzen bada.

b) Eskatzen denaren adierazpena.

c) Jakinarazpenak jasotzeko helbidea, eskatzailearen sinadura, eta data.

d) Egiten duen eskaera aintzat hartzeko nahitaezkoak diren egiaztagiriak, halakorik eskatzen denean.

13.5.– Interesdunak eskaera bidali eta jaso egin dela egiaztatzeko edozein bitarteko erabili beharko du. Eskubide horiek baliatzeko bideak errazteko, unibertsitateko erregistro nagusian, erregistro osagarrietan eta web-orrian eskaerak egiteko formularioak jarriko dira.

13.6.– Eskaerak artikulu honen laugarren puntuan zehaztutako baldintzak betetzen ez baditu, DBLO segurtasun arduradunak, fitxategiaren edo tratamenduaren pertsona erantzuleak emandako argibideak aintzat hartuz, akats horiek zuzentzeko eskatu beharko du.

13.7.– UPV/EHUk beharrezko bitartekoak jarriko ditu, datu pertsonalak erabiltzen dituzten unibertsitateko kideek interesdunari jakinaraz diezaioten zer prozedura jarraitu behar duen bere eskubideak baliatu ahal izateko.

personas vinculadas al fallecido o fallecida, por razones familiares o de hecho, podrán dirigirse a la persona «Responsable de Seguridad LOPD» con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos. La persona «Responsable de Seguridad LOPD» comunicará la información facilitada a la persona Responsable del fichero o tratamiento afectado.

13.4.– Los derechos de acceso, rectificación, cancelación y oposición se ejercerán mediante escrito dirigido a la persona «Responsable de Seguridad LOPD», a través del Registro General de la Universidad en cualquiera de las oficinas enumeradas en la Resolución de la UPV/EHU de 28 de mayo de 2007 (BOPV n.º 149, de 3 de agosto de 2007), o por cualesquiera de los medios previstos en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. La persona «Responsable de Seguridad LOPD» se encargará de hacer llegar las solicitudes recibidas a las personas Responsables de fichero o tratamiento implicados. El anterior escrito contendrá las siguientes determinaciones y requisitos:

a) Nombre y apellidos del interesado o interesada; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa de la afectada o afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente.

b) Petición en que se concreta la solicitud.

c) Domicilio a efectos de notificaciones, fecha y firma de la persona solicitante.

d) Documentos acreditativos de la petición que formula, en su caso.

13.5.– El interesado o interesada deberá utilizar cualquier medio que permita acreditar el envío y la recepción de la solicitud. Con objeto de facilitar el ejercicio de estos derechos, en el Registro General de la Universidad y sus Registros auxiliares, así como en la página web de la Universidad, se pondrán a disposición de las personas interesadas los correspondientes formularios.

13.6.– En el caso de que la solicitud no reúna los requisitos especificados en el apartado cuarto de este artículo, la persona «Responsable de Seguridad LOPD», siguiendo las indicaciones de la persona Responsable del fichero o tratamiento, deberá solicitar la subsanación de los mismos.

13.7.– La UPV/EHU articulará los mecanismos necesarios para que las personas de su organización que tienen acceso a datos de carácter personal puedan informar al afectado o afectada respecto al procedimiento a seguir para el ejercicio de sus derechos.

13.8.– Interesdunak tratamenduaren arduradun baten aurrean baliatzen dituenean bere eskubideak, horrek DBLO segurtasun-arduradunari igorri beharko dio egin zaion eskaera, berariaz ez bada aurreikusten pertsona erantzuleak eskumena emango diola tratamenduaren arduradunari datuak atzitu, zuzendu, ezereztu edo datuen aurka egiteko eskubideak baliatzeko eskaerei erantzuteko.

14. artikulua.– Datuak atzitzeko eskubidea.

14.1.– Datuak atzitzeko eskubidea da interesdunak honako hauek jakiteko duen eskubidea: inor bere datu pertsonalak tratatzen ari den, datuak zertarako ari diren tratatzen (tratatzen ari badira), datuak nondik lortu diren eta nori jakinarazi zaizkion edo jakinaraziko zaizkion.

14.2.– Datuak atzitzeko eskubidea baliatzeko eskaera egitean, interesdunak fitxategia kontsultatzeko honako sistema hauen artean aukera egin dezake, betiere fitxategiaren konfigurazioak edo ezarpenak horretarako modurik eskaintzen badio:

a) Bertaratu eta pantailan begiratuz.

b) Posta bidez idazkia, kopia edo fotokopia jasoz.

c) Posta elektronikoa edo bestelako komunikazio-sistema elektronikoren bat erabiliz.

d) Fitxategiaren konfigurazioarekin edo ezarpen materialarekin edo tratamendu-motarekin bateragarria den beste edozein prozedura jarraituz.

Edonola ere, fitxategiak kontsultatzeko goian ezarri diren sistema horiek murriztu egin daitezke fitxategiaren konfigurazioaren edo ezarpen materialaren arabera, edo tratamendu-motaren arabera, baina interesdunari eskainiko zaion sistema doakoa izango da beti, eta idatzizko jakinarazpenerako aukera eman beharko du, interesdunak hala eskatzen badu.

14.3.– Datuak atzitzeko eskaera jasotzen den egunetik kontatzen hasita, gehienez ere hilabeteko epean hartuko da haren gaineko erabakia. Eskaera baietsi egin dela jakinarazten bada, baina jakinarazpenarekin batera ez bada eskatutako informazioa ematen, jakinarazpena jasotzen den egunetik hamar eguneko epea egongo da datuak atzitzeko eskubidea betetzeko.

14.4.– Berdin da informazioa zer euskarritan ematen den, baina irakurgarria eta ulergarria izango da, eta ez du izango gailu mekaniko espezifikoak erabiltzea eskatzen duten klabe edo koderik. Informazio horrek honako hauek zehaztu beharko ditu: interesdunaren datuak, edozein lanketa edo prozesu informatikoren ondorioz lortutakoak, datuen jatorriari, erabilerari eta lagapen-hartzaileei buruzko informazioa, eta datuak gordetzearen arrazoiari buruzko zehaztapenak.

13.8.– Cuando los afectados o afectadas ejerciten sus derechos ante la persona Encargada del tratamiento, ésta deberá dar traslado de la solicitud a la persona «Responsable de Seguridad LOPD», a menos que se prevea expresamente que el Encargado atenderá, por cuenta de la persona responsable, las solicitudes de ejercicio por los afectados o afectadas de sus derechos de acceso, rectificación, cancelación u oposición.

Artículo 14.– Derecho de acceso.

14.1.– El derecho de acceso es el derecho de la afectada o afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.

14.2.– Al ejercitar el derecho de acceso, la interesada o interesado podrá optar, al formular su solicitud, por uno o varios de los siguientes sistemas de consulta del fichero, siempre que la configuración o implantación material del fichero lo permita:

a) Presencialmente mediante visualización en pantalla.

b) Escrito, copia o fotocopia remitida por correo.

c) Correo electrónico u otros sistemas de comunicaciones electrónicas.

d) Cualquier otro procedimiento que sea adecuado a la configuración o implantación material del fichero o la naturaleza del tratamiento.

No obstante, los sistemas de consulta del fichero previstos en el apartado anterior podrán restringirse en función de la configuración o implantación material del fichero o de la naturaleza del tratamiento, siempre que el que se ofrezca al afectado o afectada sea gratuito y asegure la comunicación escrita si ésta así lo exige.

14.3.– La solicitud de acceso se resolverá en el plazo máximo de un mes a contar desde la recepción de la solicitud. Si la solicitud fuera estimada pero no acompañase en la comunicación la información solicitada, el acceso se hará efectivo durante los diez días siguientes a dicha comunicación.

14.4.– La información que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. Dicha información comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como la información disponible sobre el origen de los datos, los cesionarios o cesionarias de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

14.5.– Artikulu honetan aipatzen den datuak atzitzeko eskubide hori ezingo da baliatu 12 hilabeteko epearen barruan behin baino gehiagotan, interesdunak eskubidea gehiagotan baliatzeko bidezko interesa duela egiaztatu ezean.

14.6.– I.IV.E eranskinean dago datuak atzitzeko eskaera egiteko eredua.

15. artikulua.– Datuak zuzentzeko eskubidea.

15.1.– Datuen titularrak ziur badaki fitxategi batean tratatzen diren bere datu pertsonalak okerrak direla edo osatu gabe daudela, UPV/EHUri horiek zuzentzea eska diezaioke. Datuak zuzentzeko eskaerak zehaztu beharko du zer datu diren zuzendu beharrekoak, eta zer zuzenketa egin behar den. Halaber, eskatutakoa justifikatzeko agiriak aurkeztu beharko dira.

15.2.– Unibertsitateak hamar eguneko epea izango du datuak zuzentzeko interesdunaren eskubidea betetzeko.

15.3.– Datu pertsonalak zuzenduko dira haien tratamenduak DBLOk agintzen duenari jarraitzen ez badio, eta bereziki datu horiek okerrak edo osatugabeak badira.

15.4.– Zuzendutako datuak lehenagotik beste inori utzi bazaizkio, lagapen-hartzaileari egindako zuzenketa jakinaraziko zaio epe berean, hark ere zuzenketa egin dezan, jakinarazpena jasotzen duen egunetik kontatzen hasi eta hamar eguneko epean.

15.5.– I.V.E eranskinean dago datuak zuzentzeko eskaera egiteko eredua.

16. artikulua.– Datuak ezerezteko eskubidea.

16.1.– Datuak ezerezteko eskubidea baliatzeak datu desegokiak edo neurriz gainekoak blokeatzea ekarriko du. Alabaina, administrazio publikoen, epaileen eta auzitegien esku egoten jarraituko dute, datuen tratamenduaren ondorioz sor daitezkeen erantzukizunak aintzat hartzeko, erantzukizun horien preskripzio-epeak iraun bitartean. Epe hori amaitu ondoren, datuak ezabatu egingo dira.

16.2.– Datuak ezerezteko eskaeran zehaztu beharko da zer datu ezereztu nahi diren, eta datuak ezerezteko justifikazio-agiriak aurkeztu beharko dira, halakorik eskatzen bada. Interesdunak bere datuak erabiltzearekiko adostasuna ezeztatzeko erabili ahalko du ezerezte-eskaera.

16.3.– Unibertsitateak hamar eguneko epea izango du datuak ezerezteko interesdunaren eskubidea betetzeko.

16.4.– Datuak ezabatzea bidezkoa bada, baina datu horiek ezin badira fisikoki desagerrarazi (arrazoi teknikoengatik edo erabilitako prozedura edo euskarriagatik), fitxategiaren edo tratamenduaren pertsona erantzuleak blokeatu egingo ditu datu horiek, berriro tratatu edo erabili ez daitezen. Alabaina, honako salbuespen hau

14.5.– El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que la persona interesada acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.

14.6.– Existe un modelo de formulario para el ejercicio del derecho de acceso en el anexo I.M.IV.

Artículo 15.– Derecho de rectificación.

15.1.– Cuando el titular o la titular de los datos tuvieran constancia de que sus datos de carácter personal tratados en un fichero son inexactos o incompletos, podrá solicitar a la UPV/EHU la rectificación de los mismos. La solicitud de rectificación deberá indicar a qué datos se refiere y la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado.

15.2.– La Universidad hará efectivo el derecho de rectificación del interesado en el plazo de diez días hábiles.

15.3.– Serán rectificados los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la LOPD y, en particular, cuando tales datos resulten inexactos o incompletos.

15.4.– Si los datos rectificados hubieran sido cedidos previamente, se deberá comunicar la rectificación efectuada al cesionario o cesionaria, en idéntico plazo, para que éste, también en el plazo de diez días contados desde la recepción de dicha comunicación, proceda, asimismo, a rectificar los datos.

15.5.– Existe un modelo de formulario para el ejercicio del derecho de rectificación en el anexo I.M.V.

Artículo 16.– Derecho de cancelación.

16.1.– El ejercicio del derecho de cancelación dará lugar al bloqueo de los datos inadecuados o excesivos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales para la atención de las posibles responsabilidades nacidas del tratamiento durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

16.2.– En la solicitud de cancelación, el interesado o interesada deberá indicar a qué datos se refiere, aportando al efecto la documentación que lo justifique, en su caso. La afectada o afectado podrá valerse de la solicitud de cancelación para revocar su consentimiento.

16.3.– La UPV/EHU hará efectivo el derecho de cancelación de la interesada o interesado en el plazo de diez días hábiles.

16.4.– En los casos en que, siendo procedente la supresión de los datos, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado, la persona Responsable del fichero o tratamiento procederá al bloqueo de los datos, con el fin de impedir su ulterior proceso o utilización.

egingo da: datuak iruzurra eginez edo zilegitasunik gabe jaso edo erregistratu direla egiaztatzen bada, datu horien euskarria suntsitu egingo da beti.

16.5.– Ezereztutako datuak lehenagotik beste inori utzi bazaizkio, lagapen-hartzaileari egindako ezereztea jakinaraziko zaio epe berean, hark ere ezereztu ditzan, jakinarazpena jasotzen duen egunetik kontatzen hasi eta hamar eguneko epean.

16.6.– I.IV.E eranskinean dago datuak ezerezteko eskaera egiteko eredua.

17. artikulua.– Datuen aurka egiteko eskubidea.

17.1.– Datuen aurka egiteko eskubidea da interesdunak duen eskubidea bere datu pertsonalak inork tratatu ez ditzan, edo tratatu dituenak tratatzeari utz diezaion, honako kasu hauetan:

a) Datuak tratatzeko interesdunaren adostasuna behar ez denean eta aldi berean interesdunak bere egoera pertsonalari dagokion bidezko arrazoi sendo bat daukanean datuen aurka egitea justifikatzeko, aurkakorik agintzen duen legerik egon ezean.

b) DBLOGEk 36. artikuluan ezartzen duen bezala, interesdunaren datu pertsonalen tratamendu automatizatua oinarritzat duen interesdunari buruzko erabakia hartzea denean tratamenduaren helburua.

17.2.– UPV/EHUk, datuen aurka egiteko eskaera jasotzen duen egunetik kontatzen hasita, hamar egun balioduneko epea izango du interesdunak bere eskaeran aipatzen dituen datuak tratatzeari uzteko, edo eskaera horri uko arrazoitua egiteko.

17.3.– I.VII.E eranskinean dago datuen aurka egiteko eskaera-eredua dago.

18. artikulua.– Datuak atzitzeko, zuzentzeko, ezerezteko eta datuen aurka egiteko eskaerak bideratzea.

18.1.– Datuak atzitzeko, zuzentzeko, ezerezteko edo datuen aurka jotzeko eskaerei DBLO segurtasun-arduradunak erantzungo die, eskaerak ukitzen duen fitxategian interesdunari buruzko daturik egon ala ez. Fitxategiaren edo tratamenduaren pertsona erantzuleak adierazten dionaren arabera emango du erantzuna, administrazio-jakinarazpenaren bidez, jarraian xedatzen denarekin bat etorriz. Interesdunari buruzko datu pertsonalik ez badago, horren berri emango zaio interesdunari.

18.2.– Datuak atzitzeko, zuzentzeko, ezerezteko eta datuen aurka jotzeko eskubideak baliatzeagatik ez da inolako ordainik eskatuko.

18.3.– UPV/EHUren zerbitzu juridikoari dagokio DBLO segurtasun-arduradunari eta fitxategiaren edo tratamenduaren pertsona arduradunari aholkua ematea, interesdunaren eskubideak aintzat hartzerakoan jarraitu beharreko irizpideak bateratuak izan daitezen.

Se exceptúa, no obstante, el supuesto en el que se demuestre que los datos han sido recogidos o registrados por medios fraudulentos, desleales o ilícitos, en cuyo caso la cancelación de los mismos comportará siempre la destrucción del soporte en el que aquéllos figuren.

16.5.– Si los datos cancelados hubieran sido cedidos previamente, se deberá comunicar la cancelación efectuada al cesionario o cesionaria, en idéntico plazo, para que éste, también en el plazo de diez días contados desde la recepción de dicha comunicación, proceda, asimismo, a cancelar los datos.

16.6.– Existe un modelo de formulario para el ejercicio del derecho de cancelación en el anexo I.M.VI.

Artículo 17.– Derecho de oposición.

17.1.– El derecho de oposición es el derecho del afectado o afectada a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos:

a) Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una ley no disponga lo contrario.

b) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado o afectada y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el artículo 36 del RDLOPD.

17.2.– La UPV/EHU deberá excluir del tratamiento los datos relativos a la afectada o afectado que ejercite su derecho de oposición o denegar motivadamente la solicitud del interesado o interesada en el plazo de diez días hábiles a contar desde la recepción de la solicitud.

17.3.– Existe un modelo de formulario para el ejercicio del derecho de oposición en el anexo I.M.VII.

Artículo 18.– Tramitación de las solicitudes de acceso, rectificación, cancelación y oposición.

18.1.– La solicitud de acceso, rectificación, cancelación u oposición será contestada por la persona «Responsable de Seguridad LOPD», en función de lo indicado por la persona Responsable de fichero o tratamiento con independencia de que figuren o no datos de carácter personal del interesado en los ficheros de acuerdo con lo dispuesto a continuación, mediante notificación administrativa. En el caso de que no se disponga de datos de carácter personal de los interesados o interesadas, tal circunstancia será comunicada al interesado.

18.2.– No se exigirá contraprestación alguna por el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

18.3.– Corresponderá al Servicio Jurídico de la UPV/EHU el asesoramiento a la persona Responsable de Seguridad LOPD y Responsable del fichero o tratamiento sobre la homogeneización y fijación de los criterios aplicables en la atención a los derechos del in-

Horretarako, beren ezaugarri bereziengatik edo mahaigaineratzen dituzten kontuengatik zerbitzu juridikoak aztertu beharreko eskaerak direnean, DBLO segurtasun-arduradunak zerbitzu horri igorriko dizkio datuak atzitzeko, zuzentzeko, ezerezteko eta datuen aurka jotzeko eskaerak, beharrezko dokumentazioarekin batera. Zerbitzu juridikoak egoki deritzen txosten guztiak bildu eta ahalik eta azkarren egingo du erabaki-proposamena; edozein kasutan, unibertsitateak bere gain hartutako epeak bete beharko ditu erantzuna ematerakoan.

18.4.– Eskaerak ez dira onartuko kasu hauetan:

a) Legeak edo zuzenean aplikatzeko erkidegoko zuzenbidearen arauren batek agintzen duen kasuetan.

b) Eskatzailea ez denean ez interesduna, ez haren ordezkoa (arautegi honen 13.1 artikuluan ezarritakoarekin bat).

c) Datuak atzitzeko eskubidearen kasuan, interesdunari datu horiek ezagutaraztea galarazten duen legeren bat edo zuzenean aplikatzeko erkidegoko zuzenbidearen arauren bat dagoenean. Azken hamabi hilabeteetan eskubide hori dagoeneko baliatu denean, eta ez denean egiaztatzen bidezko interesen bat dagoela eskubide hori berriro baliatzeko.

d) Datuak zuzentzeko eskubidearen kasuan, zein datu den okerra eta egin beharreko zuzenketa zein den adierazten ez denean.

e) Datuak ezerezteko eskubidearen kasuan, interesdunaren edo hirugarren baten bidezko interesei kalteren bat eragin dakiekeenean; kontratu-harreman bat dagoenean; ordainketak eta kobrantzak gestionatu behar direnean; edo datu horiek gordetzea beharrezkoa denean, UPV/EHUren helburuak modu egokian betetzeko.

18.5.– Datuak atzitzea, zuzentzea, ezereztea edo datuen haurka egitea eskatu denean, eta interesdunaren eskaera onartzea ez dela bidezkoa pentsatzen denean, horren berri emango zaio, arrazoiak azalduz. Edonola ere, UPV/EHUk justifikatu egin beharko du eskaerari egindako ukoa, eta interesdunari jakinarazi beharko dio Datuak Babesteko Euskal Bulegoaren babesa jasotzeko eskubidea duela, DBLOren 18. artikuluan ezarritakoarekin bat.

18.6.– UPV/EHUk eskaera guztiei erantzuteko eginbeharra dauka, eta eginbehar hori bete duela egiaztatzeko dokumentazioa gordeko du; alabaina, ezarritako epeetako isiltasun administratiboak adieraziko du eskaera ez dela onartu.

18.7.– Interesdunak Datuak Babesteko Euskal Bulegoaren babesa jasotzeko eskubidea baliatu ahalko du, datuak atzitzeko eskubidea baliatzen duen egunetik kontatzen hasi eta hilabete bat igaro bada edo hamar egun baliodun igaro badira datuak zuzentzeko, ezerezteko edo datuen aurka jotzeko eskubideak baliatzen

teresado. A tal efecto, la persona Responsable de Seguridad LOPD remitirá al Servicio Jurídico, junto con la documentación necesaria, aquellas solicitudes de acceso, rectificación, cancelación u oposición, que por sus características particulares o por las cuestiones en ellos planteadas, se considere que deben ser objeto de análisis jurídico específico. El Servicio Jurídico recabará los informes que estime oportunos y realizará una propuesta de resolución en el plazo más breve posible, y en cualquier caso de tal modo que se puedan cumplir los plazos de respuesta asumidos por la Universidad.

18.4.– Se rechazará la solicitud en los siguientes casos:

a) En los supuestos en que así lo prevea una ley o una norma de derecho comunitario de aplicación directa.

b) Cuando el solicitante sea una persona distinta del interesado o interesada o de su representante, de acuerdo con lo dispuesto en el artículo 13.1 del presente Reglamento.

c) En el caso o en el caso del derecho de acceso, cuando una ley o norma de derecho comunitario de aplicación directa impida revelar a los afectados el tratamiento de los datos a los que se refiera el acceso. Asimismo, cuando se haya ejercitado tal derecho de acceso en los últimos doce meses, salvo que se acredite un interés legítimo.

d) En el caso del derecho de rectificación, cuando no se indique el dato que es erróneo y la corrección que deba realizarse.

e) En el caso del derecho de cancelación, cuando se pueda causar un perjuicio a intereses legítimos de la interesada o interesado o de terceros, cuando exista una relación contractual, cuando deban gestionarse pagos y cobros, o cuando su mantenimiento sea preciso para el adecuado cumplimiento de los fines de la UPV/EHU.

18.5.– Si solicitado el acceso, la rectificación, la cancelación u oposición al tratamiento, se considera que no procede acceder a la solicitud del interesado o interesada, así se le comunicará de forma motivada. En todo caso, la UPV/EHU deberá justificar su denegación e informar al afectado de su derecho a recabar la tutela de la Agencia Vasca de Protección de Datos, conforme a lo dispuesto en el artículo 18 de la LOPD.

18.6.– La UPV/EHU deberá dar respuesta a todas las solicitudes y conservará la acreditación del cumplimiento del mencionado deber; no obstante, en el caso de silencio administrativo en los plazos fijados, se entenderá que la solicitud ha sido rechazada.

18.7.– Desde el momento en que transcurra un mes desde el ejercicio del derecho de acceso, o diez días hábiles en el caso de los derechos de rectificación, cancelación y oposición, sin que el interesado o interesada haya obtenido ninguna respuesta o cuando ésta sea negativa o no satisfactoria, el interesado podrá ejercitar su de-

dituen egunetik, eta tarte horretan inolako erantzunik jaso ez badu, edo jasotako erantzuna ezezkoa izan bada, edo erantzunarekin ados ez badago.

19. artikulua.– Balorazioak aurkaratzea.

Interesdunek beraiei buruzko hainbat alderdi ebaluatzeko helburua duten datuen tratamenduan oinarrituriko balorazioak DBLO segurtasun-arduradunaren aurrean aurkaratzeko eskubidea izango dute, eta horrek aurkaratze-eskaerak ukitzen duen fitxategi edo tratamenduaren pertsona erantzuleari helaraziko dio eskaera.

3. KAPITULUA
DATU PERTSONALAK JAKINARAZTEA

20. artikulua.– Sekretua gordetzeko betebeharra.

20.1.– UPV/EHUren datu pertsonalen tratamenduko edozein fasetan parte hartzen duen orok sekretu profesionalaren betebeharra eta datuak gordetzekoa izango ditu; betebehar horiek indarrean jarraituko dute, langileak unibertsitatearekin duen harremana hausten denean ere.

20.2.– Sekretua gordetzeko betebeharra ez betetzea zigortu egingo da indarreko legediak ezartzen duen moduan, eta diziplinazko erantzukizunak edo hirugarrenen aurrean ezar daitezkeenak ekarriko ditu.

21. artikulua.– Datuen jakinarazpenari dagozkion betebeharrak.

21.1.– Arautegi honetako 23. artikuluan berariaz ezarrita eta adierazita dauden kasuetan izan ezik, erabiltzen diren datu pertsonalak hirugarren bati jakinarazi ahalko zaizkio, baldin eta UPV/EHUren eta lagapenhartzailearen bidezko funtzioak betetzearekin zerikusi zuzena duen helbururen bat betetzeko egiten bada, eta aurretiaz interesduna jakinarazpena egitearekin ados agertzen bada, betiere arautegi honetako 11. artikuluan ezarritakoa errespetatuz.

21.2.– Datu pertsonalak hirugarren bati jakinarazteko adostasuna baliogabea izango da, interesdunak ematen zaion informazioarekin ezin duenean jakin zer datu-mota jakinarazteko baimena ematen ari den, zertarako izango diren datu horiek, eta datu horiek jasoko dituenak zer nolako jarduera duen.

21.3.– Datu pertsonalak jakinarazteko adostasuna ezeztatu ahal izango da. Arautegi honetako 11.5 artikuluan ezarritakoarekin bat etorriz datuak jakinarazteko adostasuna ezeztatzen bada, berehala eman beharko zaie horren berri lagapen-hartzaileei, interesdunaren datuak erabiltzeari utz diezaioten.

21.4.– Datu pertsonalen jakinarazpen hutsak DBLOren aginduak betetzera behartzen du jakinarazpen hori jasotzen duen oro.

recho de tutela ante la Agencia Vasca de Protección de Datos.

Artículo 19.– Impugnación de valoraciones.

Las personas interesadas tendrán derecho a impugnar valoraciones basadas en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad ante la persona Responsable de Seguridad LOPD, el cual se encargará de encauzar la solicitud a los Responsables de fichero o tratamiento afectados.

CAPÍTULO 3
COMUNICACIÓN DE DATOS DE CARÁCTER PERSONAL

Artículo 20.– Deber de secreto.

20.1.– Toda persona que intervenga en cualquier fase del tratamiento de los datos de carácter personal de la UPV/EHU está obligada al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar su relación con la Universidad.

20.2.– El incumplimiento del deber de secreto será sancionado de conformidad con lo previsto en la legislación vigente y traerá consigo las responsabilidades disciplinarias y, en su caso ante terceros, que se establezcan.

Artículo 21.– Obligaciones en las comunicaciones de datos.

21.1.– Salvo en los casos expresamente previstos e indicados en el artículo 23 del presente Reglamento, los datos de carácter personal objeto de tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas de la UPV/EHU y del cesionario con el previo consentimiento de la persona interesada respetando, en todo caso, lo establecido en el artículo 11 del presente Reglamento.

21.2.– Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite a la persona interesada no le permita conocer el tipo de datos cuya cesión se autoriza, la finalidad a la que se destinarán dichos datos, o el tipo de actividad de aquél a quien se pretenden comunicar.

21.3.– El consentimiento para la comunicación de los datos de carácter personal tiene carácter revocable, por lo que, en caso de producirse siguiendo lo establecido en el artículo 11.5 del presente Reglamento, se deberá comunicar de inmediato la revocación a los cesionarios instándoles a que cesen en el tratamiento de los datos del interesado.

21.4.– Aquél a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la LOPD.

21.5.– Jakinarazpenaren aurretik disoziazio-prozedurarik izan bada, ez da aurreko puntuetan ezarritakoa aplikatuko.

22. artikulua.– Interesdunaren adostasuna eskatzen duten datu-uzteak.

22.1.– Kanpoko erakunderen batek UPV/EHUri eskatzen badio bere esku dituen datu pertsonalak uzteko unibertsitateari bere interesekoa iruditzen zaion helburu batetarako, datu horiek uzteko hitzarmenaren izapideak egiteari ekingo zaio, aplika daitekeen unibertsitateko araudia errespetatuz. Arautegi honetako II.IV. SZ eranskinean sakonago aztertzen da kasu hori.

Hitzarmena tramitatzean txostenak eskatuko zaizkio DBLO segurtasun-arduradunari eta fitxategiaren edo tratamenduaren pertsona erantzuleari; txosten horiek lotesleak izango dira. Datuak utzi ahal izateko, fitxategiaren edo tratamenduaren pertsona erantzuleak bere txostenean egiaztatu beharko du eskatzen diren datuen jabeak aurretiaz ados agertu direla datuak uztearekin; horiek uzteko baimena eman ez duten kasuetan, eskatu egin beharko da. Adostasun-eskaera arautegi honetako 12. artikuluan ezarritakoarekin bat etorriz egingo da.

Fitxategiaren edo tratamenduaren pertsona erantzuleak egiten diren datu-uzteak erregistratuko ditu, etorkizunean datu horiek atzitzeko, zuzentzeko, ezereztekok eta datu horien aurka egiteko eskubideak benetan baliatzen direla bermatzeko. Halaber, egindako datu-uzteak fitxategiaren segurtasun-agiriko sarrera eta irteeren erregistroan agertuko dira.

22.2.– Aurreko puntuetan adierazitako prozeduraren salbuespen moduan, kanpoko erakunde batek datuak eskatzen baditu, eta UPV/EHUk pentsatzen badu kanpoko erakundeak emandako informazioa zabaltzen laguntzeko interesa duela (interes horrek zerikusia izan behar du Estatutuen arabera UPV/EHUrenak diren helburuekin), unibertsitateak informazio hori hedatu ahalko du, eta gastuak bere gain hartuko ditu.

Informazio-zabalkundea antolatzen duen UPV/EHUren unitateak (Errektoregoa, errektoreordetza, gerentzia, ikastegi, institutu edo katedrak) DBLO segurtasun-arduradunari eskatuko dio dagokion baimena, unitate horren arduradun nagusiak zabalkunderako ekimenari oniritzia eman ostean. DBLO segurtasun-arduradunak baimen hori idatziz eman ostean, unitate antolatzaileak bere gain hartuko du kanpoko erakundeak emandako informazioa bidaltzea. Informazio horrek aurretik unibertsitatearen aurkezpen-idazkia izango du, eta bertan informazio hori bidaltzea justifikatuko da.

Informazioa bidaltzeko lehenetsitako bidea posta elektronikoa izango da. Salbuespen moduan, ohiko posta erabiliko da. Horretarako, DBLO segurtasun-arduradunari egindako eskaeran behar bezala justifikatuko

21.5.– Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Artículo 22.– Cesiones que requieren el consentimiento del afectado o afectada.

22.1.– En el caso de que una entidad externa solicite a la UPV/EHU la cesión de datos de carácter personal en sus manos para un fin que la Universidad considere de interés, se deberá proceder a la tramitación del correspondiente convenio respetando lo establecido en la normativa universitaria aplicable. En el anexo II.SC.IV del presente Reglamento se profundiza en este supuesto.

En la tramitación del convenio, se solicitarán informes a la persona «Responsable de Seguridad LOPD» y a la persona Responsable del fichero o tratamiento, los cuales serán vinculantes. Para que se pueda llevar a cabo la cesión, la persona Responsable del fichero o tratamiento deberá confirmar en su informe que las personas cuyos datos se solicitan han dado previamente el consentimiento para la cesión y, si no lo han hecho, solicitar dicha autorización. La solicitud del consentimiento se realizará en el marco de lo establecido en el artículo 12 del presente Reglamento.

La persona Responsable del fichero o tratamiento procederá al registro de las cesiones de datos realizadas, con el fin de garantizar el efectivo futuro ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los interesados o interesadas. Asimismo, las cesiones realizadas serán reflejadas en el correspondiente Registro de entradas y salidas del Documento de Seguridad del fichero.

22.2.– Como salvedad al procedimiento establecido en los apartados anteriores, si se recibe una solicitud de datos por parte de una entidad externa y la UPV/EHU considere de interés colaborar en la divulgación de determinada información facilitada por la entidad externa (interés el cual siempre tendrá que estar relacionado con los fines de la UPV/EHU según sus Estatutos), la Universidad podrá llevar a cabo dicha distribución y correr con los gastos.

La unidad organizativa de la UPV/EHU implicada (Rectorado, Vicerrectorados, Gerencia, Centros, Institutos y Cátedras), tras la correspondiente aprobación de la iniciativa por su máximo responsable, solicitará el permiso correspondiente a la persona Responsable de Seguridad LOPD. Una vez de haber recibido la autorización por escrito de la persona «Responsable de Seguridad LOPD», la unidad organizativa interesada se encargará del envío de la información facilitada por la entidad externa, la cual irá introducida obligatoriamente por un escrito de presentación de la Universidad que justifique el interés de dicho envío.

El medio prioritario de distribución será el correo electrónico. Tan sólo en supuestos excepcionales, debidamente justificados en la solicitud que se realice a la persona «Responsable de Seguridad LOPD», se proce-

da ohiko posta erabiltzeko arrazoia, eta unibertsitateak bere gain hartuko ditu bidalketaren gastuak.

Halaber, unibertsitatearen web-orrian gune batzuk gorde ahalko dira bertan unibertsitateko kideentzat interesagarria den informazioa jartzeko, informazio horrek unibertsitatearekin zerikusi zuzena izan ez arren.

23. artikulua.– Interesdunaren adostasuna eskatzen ez duten datu-uzteak.

23.1.– Aurreko artikuluek ezartzen dutena alde batera utzita, unibertsitateari datuak uztea eskatzen zaionean, edo unibertsitateak datu horiek hirugarren bati utzi nahi dizkionean, honako kasu hauetan aurretiaz ez da interesdunaren adostasuna eskatuko, DBLOren 11 eta 12. artikuluekin bat etorriz:

a) Datuak uztea lege-mailako arau batek edo erkidegoko zuzenbidearen arau batek baimentzen duenean.

b) Datuak jendearen eskurako iturrietan daudenean, eta UPV/EHUk edo datu- jakinarazpena jaso duen hirugarren batek datu horiek bere legezko interesak betetzeko behar dituenean, betiere interesdunaren oinarrizko eskubideak urratzen ez badira.

c) Tratamendua askatasunez eta modu legitimoan onartutako harreman juridikoen ondorio denean, eta harreman horiek garatzeko, betetzeko zein kontrolatzeko nahitaezkoa denean tratamendua hirugarrenen fitxategiekin konektatzea. Halako kasuetan, datu-jakinarazpena legitimoa izango da, hura justifikatzen duen xedea dagoenean, eta xede hori betetzeko baino egiten ez denean.

d) Egin beharreko jakinarazpenaren jasotzailea herriaren defentsaria, fiskaltza, epaileak zein auzitegiak edo kontu-auzitegia direnean, eta datuak horiek dituzten eginkizunak gauzatzeko uzten direnean. Era berean, ez da adostasunik beharko jakinarazpenaren jasotzaileak herriaren defentsariaren edo kontu-auzitegiaren antzeko eginkizunak dituzten autonomia-erkidegoetako erakundeak direnean.

e) Datu-uztea administrazio publikoen artean egiten denean, honako hiru kasu hauetan: datu-uztearen helburua datuak geroagoko aldietan tratatzea denean, xede historiko, estatistiko eta zientifikoekin; administrazio publiko batek beste administrazio publiko batentzat bildu edo landutako datu pertsonalak direnean; datu-jakinarazpena eskumen berberak edo gai berberen inguruko eskumenak baliatzeko denean.

f) Datu-uztea disoziazio-prozeduraren ondotik egiten denean; hau da, datuak uztetik lortzen den informazioa identifikatutako norbaitekin edo identifikagarria den norbaitekin lotu ezin daitekeenean.

23.2.– Kasu horietan, datu-uzteak DBLO segurtasun-arduradunaren eta fitxategiaren edo tratamenduaren pertsona erantzulearen kontrolpean egingo dira. Zalantzarik egonez gero, nahitaezkoa izango da DBLO segurasun-arduradunari kontsulta egitea.

derá al envío por correo postal y en tal caso, los gastos serán asumidos por la propia Universidad.

Asimismo, se podrán habilitar en la web de la Universidad lugares en los que se pueda colocar información no directamente relacionada con la Universidad pero de interés para la comunidad universitaria.

Artículo 23.– Cesiones que no requieren el consentimiento del afectado o afectada.

23.1.– Al margen de lo establecido en los artículos anteriores, no se requerirá el previo consentimiento de la afectada o afectado, de acuerdo con lo establecido en los artículos 11 y 21 de la LOPD, cuando la Universidad haya sido requerida para ceder o desee facilitar dichos datos a un tercero en los siguientes supuestos:

a) La cesión está autorizada por una norma con rango de ley o una norma de derecho comunitario.

b) Se trate de datos recogidos de fuentes accesibles al público y su tratamiento es necesario para la satisfacción del interés legítimo perseguido por la UPV/EHU o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

c) El tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

d) La comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal, los Jueces o Tribunales, o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e) La cesión se produzca entre Administraciones públicas en los tres siguientes casos: cuando la cesión tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos; cuando sean datos de carácter personal que una Administración pública haya obtenido o elaborado con destino a otra; y cuando la comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.

f) Cuando la cesión se efectúe previo procedimiento de disociación, es decir, de modo que la información que se obtenga no pueda asociarse a persona determinada o determinable.

23.2.– En tales casos, las cesiones se llevarán a cabo mediante la supervisión de la persona Responsable de Seguridad LOPD y la persona Responsable del fichero o tratamiento. En caso de duda, será obligatorio consultar a la persona Responsable de Seguridad LOPD.

24. artikulua.– Datuen nazioarteko transferentzia.

24.1.– Arautegi honen arabera, datuen nazioarteko transferentzia izango da Europako Batasuneko herrialdeek eta Liechtenstein, Norvegia eta Islandiak osatzen duten Europako Ekonomia Eremutik eta Suitzatik kanpo egiten dena. Berdin da datuak utzi edo jakinarazteko diren, edo fitxategiaren edo tratamenduaren pertsona erantzuleak erabiltzeko diren.

24.2.– Datu pertsonalen nazioarteko transferentzia egin daiteke datu horiek DBLOk ematen duen segurtasun mailaren pareko segurtasuna ematen duten herrialdeetarako direnean, DBLOGEren 67, 68 eta 69. artikuluetan ezarritakoaren arabera. Bestela, aurretiaz Datuak Babesteko Espainiako Agentziaren zuzendariaren baimena lortu beharko da; eta baimen hori emateko, bermeak egokiak izan beharko dira.

24.3.– Interesdunak bere datuak uzteko zalantzarik gabeko adostasuna adierazten duenean eta datu-uztea beharrezkoa denean interesdunaren mesederako zerbitzu edo kontratu bat gauzatzeko, ez da aplikatuko aurreko puntuan ezarritakoa; halaber, ez da aplikatuko DBLOren 34. artikuluan jasotzen diren kasuetako edozeinetan.

4. KAPITULUA
TRATAMENDUAREN ARDURADUNA

25. artikulua.– Fitxategiaren barne-erantzulearen eta tratamenduaren arduradunaren arteko harremanak.

25.1.– Tratamenduaren arduradunak zerbitzu bat emateko datuak atzitzen dituenean, ez da ulertuko datuak jakinarazi direnik, betiere DBLOk eta artikulu honek ezarritakoa betetzen bada.

Tratamenduaren arduradunak ematen duen zerbitzua ordaindu beharrekoa izan daiteke edo ez, eta aldi baterako edo mugagabea izan ahal da.

Alabaina, datuak jakinarazi direla ulertuko da, datuak atzitzearen helburua atzipena egiten duenaren eta interesdunaren artean harreman berri bat ezartzea denean.

25.2.– Fitxategiaren edo tratamenduaren pertsona erantzuleak zerbitzu bat emateko kontratazioa egiten duenean, eta kontratazioak artikulu honetan ezarritakoari lotu behar zaion datu pertsonalen tratamendua eragiten duenean, fitxategiaren edo tratamenduaren pertsona erantzulearen ardura izango da berme guztiak biltzea, tratamenduaren arduradunak arautegi honetan ezarritakoa bete dezan.

25.3.– Tratamenduaren arduradunak datuak beste xede batekin erabiltzen baditu, edo DBLOren 12.2 artikuluan adierazitako kontratu-akordioak bete gabe jakinarazi edo erabiltzen baditu, tratamenduaren ar-

Artículo 24.– Transferencia internacional de datos.

24.1.– A la luz del presente Reglamento, se entiende como transferencia internacional de datos, el tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo (compuesto por los países miembros por la Unión Europea, Liechtenstein, Noruega e Islandia) y Suiza, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta de la persona Responsable del fichero o tratamiento.

24.2.– Podrán realizarse transferencias internacionales de datos de carácter personal con destino a países que proporcionen un nivel de protección equiparable a la LOPD, en función de lo establecido en los artículos 67, 68 y 69 de la RDLOPD. De otro modo, se deberá obtener la autorización previa del Director o Directora de la Agencia Española de Protección de Datos, que sólo podrá otorgarla si se obtienen las garantías adecuadas.

24.3.– Lo dispuesto en el apartado anterior no será de aplicación si la persona afectada hubiera dado su consentimiento inequívoco a la cesión, cuando la cesión fuera necesaria para la ejecución de un servicio o contrato en interés del afectado, o en cualquiera de los restantes supuestos previstos en el artículo 34 de la LOPD.

CAPÍTULO 4
ENCARGADO DEL TRATAMIENTO

Artículo 25.– Relaciones entre la persona Responsable Interno del fichero y el Encargado del tratamiento.

25.1.– El acceso a los datos por parte de un Encargado o Encargada del tratamiento que resulte necesario para la prestación de un servicio no se considerará comunicación de datos, siempre y cuando se cumpla lo establecido en la LOPD y en el presente Capítulo.

El servicio prestado por el Encargado o Encargada del tratamiento podrá tener o no carácter remunerado y ser temporal o indefinido.

No obstante, se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado o afectada.

25.2.– Cuando la persona Responsable del fichero o tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos de carácter personal sometido a lo dispuesto en este Capítulo deberá velar por que el Encargado o Encargada del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento.

25.3.– En el caso de que el Encargado o Encargada del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato al que se refiere el artículo 12.2 de la

duraduna tratamenduaren edo fitxategiaren pertsona erantzuletzat hartuko da, eta modu pertsonalean erantzungo du egin dituen arau-hausteen aurrean.

Alabaina, datuak hirugarren bati jakinaraztean, ez da inolako erantzukizunik eroriko tratamenduaren arduradunaren gain, artikulu honetan jasotakoarekin bat etorriz hirugarrenari zerbitzu bat ematea eskatu bazaio, eta fitxategiaren edo tratamenduaren pertsona erantzuleak aldez aurretik berariaz adierazi badio tratamenduaren arduradunari datuak hirugarren horri uzteko.

26. artikulua.– Zerbitzuak azpikontratatzeko aukera.

26.1.– Tratamenduaren arduradunak ezingo du hirugarren bat azpikontratatu fitxategiaren edo tratamenduaren pertsona erantzuleak agindutako tratamenduren bat burutzeko, baldin eta ez badu horretarako baimenik lortu. Kontratazioa beti fitxategiaren edo tratamenduaren pertsona erantzulearen izenean egingo da, eta haren kontura.

26.2.– Aurreko puntuan xedatutakoa alde batera utzita, baimen berririk eskatu gabe azpikontratatu ahal izango da, baldintza hauek betetzen badira:

a) Unibertsitateak eta tratamenduaren arduradunak izenpeturiko kontratuan azpikontratatu daitezkeen zerbitzuak zehazten badira, eta zerbitzu horretarako zein enpresa azpikontratatuko den zehazten bada (azken hori zehazterik badago). Kontratu horretan ez bada zerbitzua azpikontratatzeko enpresa identifikatzen, tratamenduaren arduradunak unibertsitateko kide erantzuleari enpresa hori identifikatzen duten datuak jakinarazi beharko dizkio, azpikontratazioa egin aurretik.

b) Azpikontratistaren datu pertsonalen tratamenduak fitxategiaren edo tratamenduaren pertsona erantzuleak emandako jarraibideak betetzen baditu.

26.3.– Zerbitzugintza horretan zerbitzuaren zati bat azpikontratatzeko beharra sortzen bada, eta behar hori kontratuan aurreikusi ez bada, fitxategiaren edo tratamenduaren pertsona erantzuleak bere iritzia eman beharko du horri buruz. Azken horrek erabakiko du azpikontratazio-eskaera onartu ala ez; onartzen badu, beharrezko izapideak egingo ditu azpikontratatu behar den enpresak, gutxienez, kontrataturiko enpresak hartu dituen konpromisoak bete ditzan.

27. artikulua.– Tratamenduaren arduradunak datuak gordetzea.

27.1.– Behin zerbitzu-kontratua beteta, datu pertsonalak suntsitu egin beharko dira, edo fitxategiaren edo tratamenduaren pertsona erantzuleari edo hark izendaturiko arduradun bati itzuli beharko zaizkio. Beste horrenbeste egingo da edozelako euskarri edo agirirekin ere, halakoek tratamendurako datu pertsonalen bat jaso badute.

Datuak suntsitzea ez da bidezkoa izango, legeak datu horiek gordetzea eskatzen duenean. Kasu horretan da-

LOPD, será considerado, también, la persona Responsable del fichero o tratamiento, respondiendo de las infracciones en que hubiera incurrido.

No obstante, el Encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa de la persona Responsable del fichero o tratamiento, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente Capítulo.

Artículo 26.– Posibilidad de subcontratación de los servicios.

26.1.– El Encargado o Encargada del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado la persona Responsable del fichero o tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta de la persona Responsable del fichero o tratamiento.

26.2.– No obstante lo dispuesto en el apartado anterior, será posible la subcontratación, sin necesidad de nueva autorización, siempre y cuando se cumplan los siguientes requisitos:

a) Que se especifiquen en el contrato suscrito entre la Universidad y el Encargado del tratamiento los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar. Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el Encargado o Encargada del tratamiento comunique a la persona responsable de la Universidad los datos que la identifiquen antes de proceder a la subcontratación.

b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones de la persona Responsable del fichero o tratamiento.

26.3.– Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, dicha necesidad será sometida a la consideración de la persona Responsable del fichero o tratamiento. Este último decidirá si aceptar o rechazar la solicitud y, en su caso, llevará a cabo los trámites necesarios para que la empresa a subcontratar cumpla, al menos, con los compromisos asumidos por la empresa contratada.

Artículo 27.– Conservación de los datos por el Encargado del tratamiento.

27.1.– Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos a la persona Responsable del fichero o tratamiento o al encargado o encargada que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en

tuak itzuli egingo dira, eta fitxategiaren edo tratamenduaren pertsona erantzuleak datuak gorde egiten direla bermatuko du.

27.2.– Tratamenduaren arduradunak behar bezala blokeaturik gordeko ditu datuak, fitxategiaren edo tratamenduaren pertsona erantzulearekin duen harremanaren ondorioz erantzukizunak sor litezkeen bitartean.

III. TITULUA

FITXATEGIEN BALDINTZA FORMALAK

28. artikulua.– Fitxategiak sortu, aldatu edo ezabatzea.

28.1.– Gobernu Kontseiluak hartuko ditu UPV/EHUko fitxategiak sortu, aldatu edo ezabatzeko erabakiak, eta horiek Euskal Herriko Agintaritzaren Aldizkarian argitaratuko dira. Behin argitaratu ondoren, Datuak Babesteko Euskal Bulegoari emango zaio erabakien berri, hark Datuak Babesteko Euskadiko Erregistroan erregistratu ditzan.

28.2.– Fitxategiak sortu edo aldatzeko xedapenek zehaztu beharko dute:

a) Fitxategiaren identifikazioa, bere izena adieraziz; baita bere helburuaren azalpena ere, eta zertarako erabiltzea aurreikusten den.

b) Zein pertsona edo kolektiborengandik lortu nahi diren datu pertsonalak, edo pertsona edo kolektibo horietatik nork eman behar dituen datuak nahitaez.

c) Datu pertsonalak biltzeko prozedura.

d) Fitxategiaren oinarrizko egitura.

e) Fitxategian zer-nolako datu pertsonalak sartzen diren eta datu horien deskripzioa.

f) Aurreikusitako datu pertsonalen jakinarazpenak.

g) Hirugarren herrialdeetara egin daitezkeen transferentziak, halakorik aurreikusten bada.

h) Fitxategiaren edo tratamenduaren erantzulea izango den organoa; kasu honetan, UPV/EHU.

i) Datuak atzitu, zuzendu, ezereztu eta datuen aurka egiteko eskubidea zein unitatetan erabil daitekeen; kasu honetan unibertsitateko Errektoregoan.

j) Segurtasun-neurriak, oinarrizkoak, erdi-mailakoak edo goi-mailakoak izan behar diren zehaztuta.

28.3.– Zerbitzuko arrazoiak direla eta, unibertsitateko unitateren batek datuak behar baditu, eta horiek ez badaude Datuak Babesteko Euskal Bulegoan erregistraturik dauden UPV/EHUko fitxategietan, unitate horrek DBLO segurtasun-arduradunari idatzi bat aurkeztuko dio, bertan bere eskaera adieraziz, eta eskaera egiteko dituen arrazoiak emanez. Unibertsitateko unitate horrek behar dituen datuak bildu ditzan, DBLO cuyo caso deberá procederse a la devolución de los mismos garantizando la persona Responsable del fichero o tratamiento dicha conservación.

27.2.– El Encargado o Encargada del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con la persona Responsable del fichero o tratamiento.

TÍTULO III

REQUISITOS FORMALES RELATIVOS A LOS FICHEROS

Artículo 28.– Creación, modificación y supresión de ficheros.

28.1.– La decisión de creación, modificación o supresión de ficheros de la UPV/EHU será adoptada por su Consejo de Gobierno y la resolución correspondiente será publicada en el Boletín Oficial del País Vasco. Una vez publicada tal Resolución, ésta será notificará a la Agencia Vasca de Protección de Datos para su inscripción en el Registro de Protección de Datos de Euskadi.

28.2.– Las disposiciones de creación o de modificación de ficheros deberán indicar:

a) la identificación del fichero, indicando su denominación, así como la descripción de su finalidad y usos previstos;

b) las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos;

c) el procedimiento de recogida de los datos de carácter personal;

d) la estructura básica del fichero;

e) la descripción de los tipos de datos de carácter personal incluidos en el mismo;

f) las cesiones de datos de carácter personal previstas;

g) las transferencias de datos que se prevean a países terceros, en su caso;

h) la UPV/EHU como Responsable de fichero o tratamiento;

i) el Rectorado de la Universidad como la unidad donde se puede ejercitar los derechos de acceso, rectificación, cancelación y oposición; y

j) las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

28.3.– Cuando una unidad de la Universidad necesite por razones de servicio recabar datos distintos a los mencionados en los ficheros registrados de la UPV/EHU inscritos ante la Agencia Vasca de Protección de Datos, dicha unidad realizará una solicitud a la persona Responsable de Seguridad LOPD requiriendo tal posibilidad mediante escrito motivado. En caso de reunir todas las condiciones exigidas por la ley, sus dis-

segurtasun-arduradunak, unibertsitateko Lege Zerbitzuarekin batera, beharrezko izapide guztiak egingo ditu erregistraturiko fitxategiak aldatzeko edo fitxategi berriak sortzeko, betiere legeak, lege hori garatzeko xedapenek eta arautegi honek eskatutako baldintza guztiak betetzen badira.

28.4.– Unibertsitateko Gobernu Kontseiluak 2007ko otsailaren 8an unibertsitateko datu pertsonalen fitxategiak sortu, aldatu eta ezabatzeri buruz hartutako erabakia betez aitortu zituen fitxategiak erantsi dira I.E. VIII eranskinean. Erabaki hori UPV/EHUko idazkari nagusiaren 2007ko otsailaren 28ko aginduz argitaratu zen (2007ko apirilaren 11ko EHAA, 69. zk.).

IV. TITULUA

DATUAK BABESTEAREN ARDURADUNAK

29. artikulua.– DBLO segurtasun-arduraduna.

29.1.– UPV/EHUk segurtasunaz arduratzeko pertsona bat izango du unibertsitate osoan, aurrerantzean DBLO segurtasun-arduraduna deituko duguna. Bera izango da UPV/EHUko informazioa babesteko estrategia orokorra zehaztu eta hura betearazteko ardura izango duen pertsona; bereziki, estrategia horrek datu pertsonalak babesteari buruzko lege eta arauek ezarritakoa modu egokian betetzen duela zaindu beharko du.

29.2.– DBLO segurtasun-arduradunaren eginkizunak, besteak beste, honako hauek dira:

a) Aurkezten diren eskaerak bideratzea: datuak atzitzeko, zuzentzeko, ezerezteko eta datuen aurka egiteko eskubideak baliatzeko eskaerak, adostasuna baliogabetzekoak eta balorazioak aurkaratzekoak.

b) Kanpoko erakundeei datuak uzteko eskaerak ikuskatzea.

c) Datu pertsonalak babesteari buruz sor daitezkeen zalantzak argitzea.

d) Datu pertsonalak babesteari buruzko informazioklausulak eta baimen-agiriak idaztea eta kontrolatzea.

e) Arautegi honek edo eskumena duten unibertsitate-organoek bere gain utz ditzaketen bestelako eginkizunak.

30. artikulua.– Fitxategien erantzule gorena eta fitxategien barne-erantzuleak.

30.1.– UPV/EHUk datu pertsonalak babesteari buruzko arautegia egiazki ezartzeari dagokionez, errektorea izango ezarpen horren pertsona erantzule gorena, eta unibertsitateak aitorturiko fitxategi guztien azken erantzulea ere bai.

posiciones de desarrollo y este Reglamento, la persona Responsable de Seguridad LOPD, junto con el Servicio Jurídico de la Universidad, llevarán a cabo los trámites precisos para la modificación de los ficheros inscritos o la creación de nuevos ficheros con el fin de que la citada unidad de la Universidad pueda proceder a recabar los datos que necesita.

28.4.– En el anexo I.M.VIII se adjuntan los ficheros declarados en virtud del Acuerdo adoptado por el Consejo de Gobierno de la UPV/EHU de 8 de febrero de 2007 para la creación, modificación y supresión de ficheros de datos de carácter personal de la Universidad, publicado por Resolución de 28 de febrero de 2007 del Secretario General de la UPV/EHU (BOPV n.º 69, de 11 de abril de 2007).

TÍTULO IV

RESPONSABLES EN MATERIA DE PROTECCIÓN DE DATOS

Artículo 29.– Responsable de Seguridad LOPD.

29.1.– La UPV/EHU tendrá una persona responsable de seguridad de carácter general para toda la Universidad, en adelante Responsable de Seguridad LOPD, el cual será la persona encargada de definir y velar por el cumplimiento de la estrategia global en materia de seguridad de la información de la UPV/EHU, y especialmente, la correcta adecuación de la misma a lo establecido en la normativa relativa a la protección de datos de carácter personal.

29.2.– Las funciones de la persona Responsable de Seguridad LOPD serán, entre otras, las siguientes:

a) encargarse de canalizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, las revocaciones de consentimiento y las impugnaciones de valoraciones que puedan presentarse;

b) supervisar las solicitudes de cesión de datos a entidades externas;

c) resolver cuantas dudas puedan suscitarse en relación con la protección de datos de carácter personal;

d) redactar y controlar las cláusulas informativas y documentos de autorización en relación con la protección de datos de carácter personal;

e) resto de funciones que puedan ser encomendadas por este Reglamento o las competentes instancias universitarias.

Artículo 30.– Máximo Responsable de los ficheros y Responsables Internos de fichero.

30.1.– El Rector o Rectora será la máxima persona responsable de la efectiva aplicación de la normativa en materia de protección de datos de carácter personal por parte de la UPV/EHU, y responsable último de todos los ficheros declarados por la UPV/EHU.

Alabaina, fitxategi bakoitzak fitxategiaren barne-erantzulea izango den pertsona bat izango du, eta berak erabakiko du esleitu zaion fitxategiak zer helburu, eduki eta tratamendu izango dituen; horretarako, errektorearen eskuordetzea jasoko du. Fitxategiaren barne-erantzulea den pertsonak, esleitu zaion fitxategiari dagokionez, legeak edo arautegi honek fitxategiaren edo tratamenduaren pertsona erantzuleari esleitzen dizkion eginkizunak beteko ditu.

30.2.– Fitxategiaren barne-erantzulea den pertsonaren eginkizunak izango dira:

a) fitxategiaren segurtasuna zaintzea; beraz, esleitu zaion fitxategian segurtasun informatikoarekin eta datuak babestearekin zerikusirik duen unibertsitateko arautegia ezartzeaz arduratuko da;

b) beharrezko ekintzak burutzea, UPV/EHUko kideek, bereziki Errektogo, errektoreordetza, ikastegi, sail, unibertsitateko ikerketa-institutu, unibertsitateko zerbitzu edo beste organo batzuetako datu pertsonalen babeserako koordinatzaileek, beren fitxategiarekin loturiko eginkizunen garapenean eragina duten arauak ezagutu ditzaten, baita arau horiek ez betetzeak ekar ditzakeen ondorioak ere;

c) Arautegi honek edo eskumena duten unibertsitate-organoek bere gain utz ditzaketen bestelako eginkizunak.

30.3.– Pertsona bera izan daiteke hainbat fitxategiren barne-erantzulea.

31. artikulua.– Segurtasun Informatikorako eta Dokumentuen Gestiorako Batzordea.

31.1.– Fitxategien barne-erantzuleek batzorde bat izendatuko dute beren fitxategien «segurtasun-arduradun» (DBLOGEren definizioaren arabera). Batzorde hori Segurtasun Informatikorako eta Dokumentuen Gestiorako Batzordea izango da. Beraz, batzorde hori arduratuko da UPV/EHUren fitxategi guztietan ezar daitezkeen segurtasun-neurriak koordinatu eta kontrolatzeaz, eta horretarako bere ustez egokiak diren pertsonen laguntza izango du.

31.2.– Batzorde hori osatzen dutenak hauek izango dira:

– Informazio eta Komunikazio-Teknologien gerenteordea (edo gerenteak izendaturiko gerenteordea).

– DBLO segurtasun-arduraduna.

– Unibertsitateko informatika-gune bakoitzeko pertsona bat.

– Idazkaritza Nagusiko artxiboko teknikaria.

– Lege Zerbitzuko pertsona bat.

32. artikulua.– Datuak Babesteko Batzordea.

No obstante, cada fichero tendrá una persona Responsable Interno de fichero, que por delegación del Rector o Rectora, decidirá sobre la finalidad, contenido y tratamiento del fichero que se le asigne. La persona Responsable Interno del fichero cumplirá las funciones asignadas por la ley o este Reglamento a la persona Responsable del fichero o tratamiento en relación al fichero que le ha sido adjudicado.

30.2.– La persona Responsable Interno del fichero será la encargada de:

a) la seguridad del fichero, por lo que se responsabilizará de la implantación de la normativa universitaria relacionada con la seguridad informática y la protección de datos en relación con el fichero que le ha sido asignado;

b) llevar a cabo las acciones necesarias para que el personal de la UPV/EHU, especialmente los Coordinadores o Coordinadoras de la protección de datos de carácter personal de Rectorado, Vicerrectorado, Centro, Departamento, Instituto Universitario de Investigación, servicio u organismo universitario, conozcan las normas que afectan al desarrollo de sus funciones en relación con su fichero, así como las consecuencias en que pudieran incurrir en caso de incumplimiento;

c) resto de funciones que puedan ser encomendadas por este Reglamento o las competentes instancias universitarias.

30.3.– Una misma persona podrá ser Responsable Interno de varios ficheros.

Artículo 31.– Comité de Seguridad Informática y Gestión Documental.

31.1.– Los Responsables Internos de los ficheros designarán a un comité, la «Comité de Seguridad Informática y Gestión Documental», como «Responsable de Seguridad» (según definición del RDLOPD) de sus ficheros. Por lo tanto, dicho comité será el encargado de coordinar y controlar las medidas de seguridad aplicables en relación con todos los ficheros de la UPV/EHU y para ello, podrá apoyarse en las personas que estime oportuno.

31.2.– La composición de este Comité será la siguiente:

– El Vicegerente o Vicegerenta de Tecnologías de la Información y las Comunicaciones (o Vicegerente designado por el Gerente).

– La persona Responsable de Seguridad LOPD.

– Una persona de cada Centro de Informática de la Universidad.

– El o la técnico de Archivo de Secretaría General.

– Una persona del Servicio Jurídico.

Artículo 32.– Comisión para la Protección de Datos.

32.1.– Batzorde hori gutxienez sei hilabetez behin bilduko da, arautegi hau benetan ezar dadin kontrol- eta koordinazio-lanak burutu asmoz, eta datuak babesteari dagokionez UPV/EHUren jarraibideak ezarri asmoz.

32.2.– Batzorde hori osatzen dutenak hauek izango dira:

– Baliabide Orokorren gerenteordea (edo gerenteak izendaturiko gerenteordea).

– DBLO segurtasun-arduraduna.

– DBLO segurtasun-arduradunaren proposamenari jarraituz, errektoreak izendaturiko fitxategien barne-erantzuleak (bi pertsona erantzule).

– Idazkaritza Nagusiko burua.

– Lege Zerbitzuko pertsona bat.

– Unibertsitate-ikastegiko administratzailea, gerenteak izendaturikoa.

– Campuseko idazkaria, idazkari nagusiaren proposamenari jarraiki errektoreak izendaturikoa.

32.3.– Datuak Babesteko Batzordeak eginkizun hauek izango ditu, besteak beste:

a) Arautegi honen ezarpena ikuskatzea eta neurriak bultzatzea, benetan aplikatzea lor dadin.

b) Arautegiak beharrezko dituen eguneratzeak proposatzea, eta proposamenen onarpena bultzatzea unibertsitate-organo eskudunen aurrean.

c) DBLO segurtasun-arduradunaren aurrean aurkezten diren eskaeren jarraipena egitea; hain zuzen ere, datuak atzitzeko, zuzentzeko, ezerezteko eta datuen aurka egiteko eskubideak baliatzeko eskaerena eta adostasuna baliogabetzeko nahiz balorazioak aurkaratzeko eskaerena.

d) Arautegi honek edo eskumena duten unibertsitate-organoek bere gain utz ditzaketen bestelako eginkizunak.

33. artikulua.– Errektorego, errektoreordetza, ikastegi, sail, unibertsitateko ikerketa-institutu, unibertsitateko zerbitzu edo beste organo batzuetako datu pertsonalen babeserako koordinatzailea.

Errektorego, errektoreordetza, ikastegi, sail, unibertsitateko ikerketa-institutu, unibertsitateko zerbitzu edo bestelako organo baten erantzule nagusiak bere gain hartuko du ardura, unibertsitateko datu pertsonalak babesteari buruzko arautegia zabaldu, ezarri eta benetan betetzen dela bermatzeko, berari dagokion arloan, eta unibertsitateko datu pertsonalak babesteko gainerako erantzuleekin koordinatuz eta lankidetzan arituz; era berean, lan horiek egiteko beste pertsona batzuk izenda ditzake, baina bere erantzukizuna horien gain utzi gabe.

32.1.– Esta Comisión se reunirá al menos semestralmente con el objeto de llevar a cabo el control y la coordinación de la efectiva implantación del presente Reglamento y establecer las pautas de actuación de la UPV/EHU en cuestión de protección de datos.

32.2.– La composición de esta Comisión será la siguiente:

– El Vicegerente o Vicegerenta de Recursos Generales (o Vicegerente designado por el Gerente).

– La persona Responsable de Seguridad LOPD.

– Dos personas Responsables Internos de Fichero designados por el Rector o Rectora a propuesta de la persona Responsable de Seguridad LOPD.

– El Jefe o Jefa de Secretaría General.

– Una persona del Servicio Jurídico.

– Un Administrador o Administradora de Centro universitario designado por el Gerente o Gerenta.

– Un Secretario o Secretaria de Campus designado por el Rector o Rectora a propuesta del Secretario o Secretaria General.

32.3.– Las funciones de la Comisión para la Protección de Datos, entre otras, serán las siguientes:

a) supervisar la implantación del presente Reglamento y promover medidas para la consecución de su efectiva aplicación;

b) proponer e impulsar la aprobación de las actualizaciones necesarias del presente Reglamento ante los órganos universitarios competentes;

c) realizar un seguimiento de los derechos de acceso, rectificación, cancelación y oposición, revocación del consentimiento e impugnación de valoraciones que se presenten ante la persona Responsable de Seguridad LOPD;

d) resto de funciones que puedan ser encomendadas por este Reglamento o las competentes instancias universitarias.

Artículo 33.– Coordinador o Coordinadora de la protección de datos de carácter personal de Rectorado, Vicerrectorado, Centro, Departamento, Instituto Universitario de Investigación, servicio u otro organismo universitario.

El máximo o máxima responsable del Rectorado, Vicerrectorado, Centro, Departamento, Instituto Universitario de Investigación, servicio u otro organismo universitario será la persona encargada de difundir, implantar y garantizar la efectiva aplicación de la normativa relativa a la protección de datos de carácter personal de la Universidad en el ámbito que le corresponda, en coordinación y colaboración con el resto de responsables en materia de protección de datos de carácter personal de la Universidad, y pudiendo designar a su vez a otras personas para estar tareas sin que ello implique una delegación de su responsabilidad.

V. TITULUA

SEGURTASUN NEURRIAK

1. KAPITULUA
EZARTZEKO NEURRI OROKORRAK

34. artikulua.– Segurtasun-mailak.

34.1.– Hiru segurtasun-maila ezarriko dira: oinarrizkoa, erdikoa eta goikoa. Maila horiek fitxategi eta tratamenduei aplikatuko zaizkie, automatizatuei nahiz ez-automatizatuei, tratatzen den informazioa nolakoa den aintzat hartuta, eta kontuan izanik informazio hori isilpean eta osorik gordetzeko beharra norainokoa den.

34.2.– Datu pertsonalen fitxategi edo tratamendu guztiek hartu beharko dituzte oinarrizko segurtasun-neurriak.

34.3.– Oinarrizko segurtasun-neurri horiez gain, erdi-mailako segurtasun-neurriak ezarri beharko dira datu pertsonalen fitxategi edo tratamendu hauetan:

– Arau-hauste administratibo eta penalak egitearen inguruko datuak dituztenetan.

– Zerga-administrazioen, finantza-erakundeen, ondare-kaudimenaren eta kredituaren gaineko informazio-zerbitzua ematen duten erakundeen eta Gizarte Segurantzaren erakunde kudeatzaileen eta zerbitzu komunen ardurapean dauden fitxategietan, eta lan-istripu eta gaixotasun profesionaletarako Gizarte Segurantzaren mutuetan.

– Herritarren ezaugarriak edo nortasuna definitzen dituzten datuak izanik, horien nortasunaren edo portaeraren hainbat alderdi baloratzeko aukera ematen duten datu-multzoak dituzten fitxategietan.

34.4.– Oinarrizko eta erdi-mailako segurtasun-neurriez gain, goi-mailakoak ezarriko dira datu pertsonalen fitxategi edo tratamendu hauetan:

– Ideologiari, sindikatu-bazkidetzari, erlijioari, sinesmenei, arrazari, osasunari edo bizitza sexualari buruzko datuak dituzten fitxategietan.

– Interesdunen adostasunik gabe, polizia-xedeetarako bildutako datuak dituzten fitxategietan.

– Genero-indarkeriaren ondoriozko datuak dituzten fitxategietan.

34.5.– Oinarrizko mailako segurtasun-neurriez gain eta erdi-mailakoez gain DBLOGEren 103. artikuluak jasotzen duen goi-mailako segurtasun-neurria aplikatuko da jendearen eskurako komunikazio elektronikoetarako zerbitzuak eskaintzen dituzten operadoreen ardurapean dauden fitxategietan, edo trafiko- eta lo-

TÍTULO V

MEDIDAS DE SEGURIDAD

CAPÍTULO 1
MEDIDAS DE APLICACIÓN GENERAL

Artículo 34.– Niveles de seguridad.

34.1.– Se establecen tres niveles de seguridad - básico, medio y alto -, que deben aplicarse a los ficheros y tratamientos, tanto automatizados como no automatizados, atendiendo a la naturaleza de la información tratada y en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

34.2.– Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

34.3.– Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de carácter personal:

– Los relativos a la comisión de infracciones administrativas o penales.

– Aquellos de los que sean responsables las Administraciones Tributarias, las entidades financieras, las entidades dedicadas la prestación de servicios de información sobre solvencia patrimonial y crédito, las Entidades Gestoras y Servicios Comunes de la Seguridad Social, y las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

– Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de las ciudadanas o ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

34.4.– Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

– Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

– Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

– Aquéllos que contengan datos derivados de actos de violencia de género.

34.5.– A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico

kalizazio-datuen inguruko komunikazio elektronikoetarako sare publikoak ustiatzen dituzten operadoreen ardurapean dauden fitxategietan.

34.6.– Ideologiari, sindikatu-bazkidetzari, erlijioari, sinesmenei, arrazari, osasunari edo bizitza sexualari buruzko datuak dituzten fitxategiei dagokienez, nahikoa izango da oinarrizko segurtasun-neurriak ezartzea, kasu hauetan:

a) Datuak banketxeetara diru-transferentzia egiteko baino ez direnean erabiltzen, interesdunak banketxe horietako bazkideak edo kideak direnean.

b) Datu-fitxategi edo datu-tratamendu ez-automatizatuak direnean, eta beren helburuarekin zerikusirik ez duten halabeharrezko datuak edo datu osagarriak dauzkatenean.

34.7.– Eginkizun publiko bat bete behar denean, osasunari buruzko datuak dituzten fitxategi edo tratamenduetan oinarrizko segurtasun-neurriak ezarri ahalko dira, minusbaliotasun-maila baizik aipatzen ez denean, edo minusbaliotasuna zein baliaezintasuna aitortzeko interesdunaren adierazpen hutsa baizik ez denean.

34.8.– Gorago deskribatu diren maila bakoitzerako neurriak bete beharreko gutxieneko baldintzak dira, kalterik egin gabe kasu bakoitzean ezar daitezkeen indarreko lege- edo arau-xedapen espezifikoei, edo fitxategi edo tratamenduaren pertsona erantzulearen ekimenei.

34.9.– Titulu honetan xedatutakoa errazago bete dadin, informazio-sistema batean sistema nagusiko segurtasun-neurriez bestelako neurriak ezartzea beharrezkoa bada, sistema horretako fitxategi edo tratamenduen helburuak edo erabilerak edo dituzten datuen ezaugarriek hala eskatzen dutelako, sistema nagusitik bereizi ahal izango dira, eta kasu bakoitzean dagokien segurtasun-mailaren araberako neurriak aplikatu ahal izango zaizkie, betiere ukitutako datuak eta datuak atzitzerik duten erabiltzaileak zehaztu badaitezke, eta hori segurtasun-agirian idatziz jasotzen bada.

34.10.– DBLOGEk agintzen duenaren arabera fitxategi automatizatuetan eta ez-automatizatuetan aplika daitezkeen segurtasun-neurriei buruzko laburpen-koadroak daude, hurrenez hurren, I.IX.E eta I.X.E. eranskinetan.

35. artikulua.– Tratamenduaren arduraduna.

35.1.– Fitxategi edo tratamenduaren pertsona erantzuleak bere lokalean zerbitzuren bat ematen duen tratamenduaren arduradunari ahalbidea ematen badio datuak, edo datuen euskarriak, edo datuak tratatzen dituen informazio-sistemaren baliabideak atzitzeko, idatziz jaso beharko da hori aipatutako erantzulearen segurtasun-agirian, eta tratamenduaren arduradunaren langileek aipatutako agirian ezarritako segurtasun-neurriak betetzeko konpromisoa hartuko dute.

y medio, la medida de seguridad de nivel alto contenida en el artículo 103 del RDLOPD.

34.6.– En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que las afectadas o afectados sean asociados o miembros.

b) Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

34.7.– También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado o afectada, con motivo del cumplimiento de deberes públicos.

34.8.– Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase la persona Responsable del fichero o tratamiento.

34.9.– A los efectos de facilitar el cumplimiento de lo dispuesto en este Título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios o usuarias con acceso a los mismos, y que esto se haga constar en el Documento de Seguridad.

34.10.– En el anexo I.M.IX y anexo I.M.X se incluye un cuadro resumen sobre las medidas de seguridad aplicables a los ficheros automatizados y no automatizados, respectivamente, en función de lo establecido por el RDLOPD.

Artículo 35.– Encargado del tratamiento.

35.1.– Cuando la persona Responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un Encargado del tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el Documento de Seguridad de dicha persona Responsable, comprometiéndose el personal del Encargado del tratamiento al cumplimiento de las medidas de seguridad previstas en el citado documento.

Urruneko atzipena bada, eta tratamenduaren arduradunari datu horiek pertsona erantzulearenak ez diren sistema edo euskarrietan sartzea debekatu bazaio, debeku hori idatziz jaso beharko da pertsona erantzulearen segurtasun-agirian, eta tratamenduaren arduradunaren langileek aipatutako agirian ezarritako segurtasun-neurriak betetzeko konpromisoa hartuko dute.

35.2.– Tratamenduaren arduradunak zerbitzua bere lokaletan ematen badu (hau da, fitxategiaren edo tratamenduaren pertsona erantzulearenak ez diren lokaletan), segurtasun-agiri bat egin beharko du, edo lehendik egina izan lezakeen agiria osatu, fitxategia edo tratamendua eta horien pertsona erantzulea identifikatuz, eta tratamendu horri dagozkion segurtasun-neurriak ezarriz.

35.3.– Edonola ere, tratamenduaren arduradunaren datu-atzipena arautegi honetako segurtasun-neurrien menpe egongo da.

36. artikulua.– Zerbitzuak datu pertsonalak atzitu gabe ematea.

Datu pertsonalak tratatzea eskatzen ez duten lanak egiteko, fitxategiaren edo tratamenduaren pertsona erantzuleak neurri egokiak hartuko ditu langileei datu pertsonalen atzipena mugatzeko; baita datuen euskarrien eta informazio-sistemaren baliabideen atzipena mugatzeko ere.

UPV/EHUz kanpoko pertsonala bada, zerbitzuak emateko kontratuan berariaz jasoko dira datu pertsonalak atzitzeko debekua, eta pertsonalak daukan betebeharra zerbitzua emateagatik ezagutu ditzakeen datu pertsonalak sekretuan gordetzeko.

37. artikulua.– Baimenak eskuordetzea.

Titulu honetan fitxategiaren edo tratamenduaren pertsona erantzuleari esleitzen zaizkion baimenak eskuordetu ahal izango zaizkio horretarako izendatzen denari. Segurtasun-agirian baimen horiek emateko gaitu diren pertsonak eta eskuordetzea jasotzeko izendatu direnak adieraziko dira. Izendapen horrek ez du inola ere esan nahiko fitxategiaren edo tratamenduaren pertsona erantzuleari dagokion erantzukizuna eskuordetzen denik.

38. artikulua.– Komunikazio-sareen bidez datuak atzitzea.

Komunikazio-sareen bidezko datuen atzipenei eskatuko zaizkien segurtasun-neurriek bermatu beharreko segurtasun-maila atzipen lokalekoek bermatu beharrekoaren parekoa izango da (sare horiek publikoak izan ala ez), arautegi honen 34. artikuluan ezarritako irizpideak jarraituz.

39. artikulua.– Fitxategiaren edo tratamenduaren pertsona erantzulearen eta tratamenduaren arduradunaren lokalez kanpoko lan-araudia.

Cuando dicho acceso sea remoto habiéndose prohibido al Encargado del tratamiento incorporar tales datos a sistemas o soportes distintos de los de la persona Responsable, este último deberá hacer constar esta circunstancia en el Documento de Seguridad de la persona Responsable, comprometiéndose el personal del Encargado del tratamiento al cumplimiento de las medidas de seguridad previstas en el citado documento.

35.2.– Si el servicio fuera prestado por el Encargado del tratamiento en sus propios locales, ajenos a los de la persona Responsable del fichero o tratamiento, deberá elaborar un Documento de Seguridad o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y la persona Responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

35.3.– En todo caso, el acceso a los datos por el Encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este Reglamento.

Artículo 36.– Prestaciones de servicios sin acceso a datos de carácter personal.

La persona Responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos de carácter personal, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos de carácter personal.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos de carácter personal y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

Artículo 37.– Delegación de autorizaciones.

Las autorizaciones que en este Título se atribuyen la persona Responsable del fichero o tratamiento podrán ser delegadas en las personas designadas al efecto. En el Documento de Seguridad deberán constar las personas habilitadas para otorgar estas autorizaciones así como aquellas en las que recae dicha delegación. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde a la persona Responsable del fichero o tratamiento.

Artículo 38.– Acceso a datos a través de redes de comunicaciones.

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 34 del presente Reglamento.

Artículo 39.– Régimen de trabajo fuera de los locales de la persona Responsable del fichero o tratamiento o Encargado o Encargada del tratamiento.

39.1.– Datu pertsonalak gailu eramangarrietan gorde ahal izateko, edo fitxategiaren edo tratamenduaren pertsona erantzulearen nahiz tratamenduaren arduradunaren lokaletatik kanpo tratatu ahal izateko, fitxategiaren edo tratamenduaren pertsona erantzuleak aurretiaz baimena eman beharko du, eta tratatzen den fitxategi motari dagokion segurtasun-maila bermatu beharko da beti.

39.2.– Aurreko paragrafoan aipatutako baimen hori segurtasun-agirian jaso beharko da, eta baimenaren erabiltzailea edo erabiltzaile-profila ezarri ahalko da, baimenaren baliotasun-epea zehaztuz.

40. artikulua.– Fitxategi iragankorrak edo aldi baterako lanetarako dokumentuen kopiak.

40.1.– Fitxategi iragankorrek edo aldi baterako lanak edo lan osagarriak egiteko baizik sortu ez diren dokumentuen kopiek bete beharreko segurtasun-neurriak arautegi honen 34. artikuluan ezarritakoaren arabera dagozkienak izango dira.

40.2.– Fitxategi iragankorrak edo aldi baterako lanei dagozkien kopiak ezabatu edo suntsitu egingo dira, horiek sortzea eragin zuen helburua betetzeko beharrezkoak izateari uzten diotenean.

2. KAPITULUA
SEGURTASUN-AGIRIA ETA AUDITORETZA

41. artikulua.– Segurtasun-agiria.

41.1.– UPV/EHUk segurtasunari buruzko araudia ezarriko du, teknika eta antolakuntzari buruzko neurriak jasoko dituen agiri baten bidez; agiri hori bat etorriko da indarreko segurtasun-araudiarekin. Datu pertsonalak eta informazio-sistemak atzitu ahal dituztenek derrigor bete beharko dute agiri horretan ezartzen dena.

41.2.– Agiriak, gutxienez, honako alderdi hauek jaso beharko ditu:

a) Agiria zer esparrutan aplikatuko den eta zeintzuk diren babestutako baliabideak.

b) Arautegi honetan eskatzen den segurtasun-maila bermatzeko neurriak, arauak, jarduteko prozedurak, erregela eta estandarrak zeintzuk izango diren.

c) Fitxategietako datu pertsonalak tratatzeari dagokionez, langileek zer eginkizun eta betebehar dituzten.

d) Datu pertsonalak dituzten fitxategien egitura, eta horiek tratatzen dituzten informazio-sistemen deskribapena.

e) Gorabeherak jakinarazteko, gestionatzeko eta horien aurrean erantzuteko prozedura.

f) Segurtasun-kopiak egiteko prozedura eta datu-fitxategi edo datu-tratamendu automatizatuetako datuak berreskuratzekoa.

39.1.– Cuando los datos de carácter personal se almacenen en dispositivos portátiles o se traten fuera de los locales de la persona Responsable de fichero o tratamiento, o del Encargado o Encargada del tratamiento será preciso que exista una autorización previa de la persona Responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

39.2.– La autorización a la que se refiere el párrafo anterior tendrá que constar en el Documento de Seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

Artículo 40.– Ficheros temporales o copias de trabajo de documentos.

40.1.– Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios establecidos en el artículo 34 del presente Reglamento.

40.2.– Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

CAPÍTULO 2
DOCUMENTO DE SEGURIDAD Y AUDITORIA

Artículo 41.– Documento de Seguridad.

41.1.– La UPV/EHU implantará la normativa de seguridad mediante un documento que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente. Dicho documento será de obligado cumplimiento para el personal con acceso a datos de carácter personal y sistemas de información.

41.2.– El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.

c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Dokumentu eta euskarriak garraiatzeko hartu behar diren neurriak, dokumentu eta euskarriak suntsitzeko hartu behar direnak, edo, behar izanez gero, horiek berriro erabiltzeko hartu behar direnak.

h) Datu-fitxategi edo datu-tratamendu ez-automatizatuei dagozkienez, hartu diren segurtasun-neurriak.

i) «Segurtasun-arduraduna» denaren identifikazioa; hau da, Segurtasun Informatikorako eta Dokumentuen Gestiorako Batzordearena.

j) Agirian bertan ezarritakoa betetzen dela egiaztatzeko aldian behin egin behar diren kontrolak.

41.3.– Datuak hirugarrenen enkarguz tratatzen badira, segurtasun-agiriak identifikatu egin beharko ditu enkargu moduan tratatzen diren fitxategi eta tratamenduak, eta berariaz adierazi beharko du zein kontratu edo agiritan arautzen diren enkarguaren baldintzak, baita enkarguaren erantzulea eta indarraldia zein den ere.

41.4.– Fitxategi edo tratamendu bateko datu pertsonalak tratamenduaren arduradunaren sisteman baino ez badira sartzen eta tratatzen, fitxategiaren edo tratamenduaren pertsona erantzuleak segurtasun-agirian idatzi beharko du hori. Aipatutako hori fitxategi edo tratamenduaren pertsona erantzulearen fitxategi edo tratamendu batzuekin edo guztiekin gertatzen denean, tratamenduaren arduradunari eskuordetu ahalko zaio segurtasun-agiria eramatea, baliabide propioetan dituen datuak izan ezean. Gertaera hori berariaz adierazi beharko da Datu Pertsonalak Babesteari buruzko abenduaren 13ko 15/1999 Lege Organikoaren 12. artikuluaren babespean eginiko kontratuan, eta ukitutako fitxategi edo tratamenduak zehaztu beharko dira. Kasu horretan, arautegi honetan ezarritako betetzeko, arduradunaren segurtasun-agiriari jarraituko zaio.

41.5.– Segurtasun-agiria uneoro eguneraturik egon beharko da, eta berrikusi egin beharko da aldaketa garrantzitsuak gertatzen direnean informazio-sisteman, tratamendu-sistemaren erabileran eta antolakuntzan eta fitxategi eta tratamenduetako informazioaren edukian; halaber, aldian behingo kontrolen ondorioz aldaketak egon direnean ere berrikusi egin beharko da. Edozein kasutan, aldaketa bat garrantzitsua dela ulertuko da, ezarritako segurtasun-neurrietan eragina izan dezakeenean.

41.6.– Segurtasun-agiriaren edukia datu pertsonalen segurtasunari buruzko indarreko xedapenetara egokitu beharko da uneoro.

42. artikulua.– Auditoretza.

42.1.– Segurtasun-neurrien maila ertainetik aurrera, gutxienez bi urtean behin kanpo- zein barne-auditoretza egin beharko da, datuei buruzko informazio-sistemak

g) Las medidas que sea necesario adoptar para el transporte de documentos y soportes, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

h) Las medidas de seguridad adoptadas respecto de los ficheros o tratamientos no automatizados.

i) La identificación de la persona «responsable de seguridad», es decir, el Comité de Seguridad Informática y Gestión Documental.

j) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

41.3.– Cuando exista un tratamiento de datos por cuenta de terceros, el Documento de Seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de Encargado o Encargada con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

41.4.– En aquellos casos en los que datos de carácter personal de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del Encargado, la persona Responsable del fichero o tratamiento deberá anotarlo en el Documento de Seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos de la persona Responsable del fichero o tratamiento, podrá delegarse en el Encargado del tratamiento la llevanza del Documento de Seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de los datos de carácter personal, con especificación de los ficheros o tratamientos afectados. En tal caso, se atenderá al Documento de Seguridad del Encargado al efecto del cumplimiento de lo dispuesto por este Reglamento.

41.5.– El Documento de Seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

41.6.– El contenido del Documento de Seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

Artículo 42.– Auditoria.

42.1.– A partir del nivel medio de medidas de seguridad, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al

eta datuak tratatu eta gordetzeko instalazioak aztertu eta titulu honetan ezarritakoa betetzen dela egiaztatzeko. Salbuespen moduan auditoretza egin beharko da, informazio-sistemak egokituak, egokiak eta eraginkorrak direla egiaztatzeko ezarritako segurtasun-neurriak betetzean eragina duten aldaketak egiten badira informazio-sistema horietan. Auditoretza horrek aurreko paragrafoan adierazitako bi urteko zenbaketa hasiko du.

42.2.– Auditoretzak egindako txostenak irizpidea eman behar du erabilitako neurriak eta kontrolak arautegi honi, legeari eta legea garatzen duten arauei egokitzen zaizkien ala ez erabakitzeko; halaber, txosten horrek hutsuneak identifikatu behar ditu, eta hutsune horiek zuzendu edo osatzeko beharrezko neurriak proposatu beharko ditu. Era berean, datuak eta gorabeherak jakinarazi eta oharrak egin behar ditu, emandako irizpenak eta egindako proposamenak zertan oinarritzen diren erakusteko.

42.3.– Auditoretzaren txostenak DBLO segurtasun-arduradunak aztertuko ditu, eta azterketaren ondorioak jakinaraziko dizkie fitxategien barne-erantzuleei, Segurtasun Informatikorako eta Dokumentuen Gestiorako Batzordeari eta Datuak Babesteko Batzordeari, horiek neurri zuzentzaile egokiak har ditzaten. Gainera, txosten horiek Datuak Babesteko Euskal Bulegoaren esku geratuko dira.

3. KAPITULUA
DATU-FITXATEGI ETA DATU-TRATAMENDU AUTOMATIZATUEI EZAR DAKIZKIEKEEN SEGURTASUN-NEURRIAK

LEHENENGO ATALA
OINARRIZKO SEGURTASUN NEURRIAK

43. artikulua.– Langileen eginkizunak eta betebeharrak.

43.1.– Segurtasun-agirian argi eta garbi zehaztu eta dokumentatuko dira datu pertsonalak eta informazio-sistemak atzitu ahal dituzten erabiltzaileen edo erabiltzaile-profilen eginkizun eta betebeharrak. Fitxategi edo tratamenduaren pertsona erantzuleak eskuordetzen dituen kontrol-eginkizunak eta baimenak ere zehaztuko dira.

43.2.– Fitxategi edo tratamenduaren pertsona erantzuleak beharrezko neurriak hartuko ditu langileei beren eginkizunen garapenean eragina duten segurtasun-neurriak modu ulergarrian ezagutarazteko, eta neurri horiek bete ezean izan ditzaketen ondorioak jakinarazteko.

44. artikulua.– Gorabeheren erregistroa.

Datu pertsonalei eragiten dieten gorabeherak jakinarazi eta gestionatzeko prozedura bat egon beharko da, eta erregistro bat ezarri beharko da honako hauek adierazteko: nolako gorabehera izan den, noiz gertatu edo antzeman den, gorabeheraren jakinarazpena nork

menos cada dos años, a una auditoria interna o externa que verifique el cumplimiento del presente Título. Con carácter extraordinario deberá realizarse dicha auditoria siempre que se realicen modificaciones en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoria inicia el cómputo de dos años señalado en el párrafo anterior.

42.2.– El informe de auditoria deberá dictaminar sobre la adecuación de las medidas y controles tanto al presente Reglamento como a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

42.3.– Los informes de auditoria serán analizados por la persona Responsable de Seguridad LOPD, que elevará las conclusiones a los Responsables Internos de los Ficheros, al Comité de Seguridad Informática y Gestión Documental, y a la Comisión para la Protección de Datos, con el fin de que adopten las medidas correctoras adecuadas. Asimismo, quedarán a disposición de la Agencia Vasca de Protección de Datos.

CAPÍTULO 3
MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS Y TRATAMIENTOS AUTOMATIZADOS

SECCIÓN PRIMERA
MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO

Artículo 43.– Funciones y obligaciones del personal.

43.1.– Las funciones y obligaciones de cada uno de los usuarios y usuarias o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el Documento de Seguridad. También se definirán las funciones de control o autorizaciones delegadas por la persona Responsable del fichero o tratamiento.

43.2.– La persona Responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Artículo 44.– Registro de incidencias.

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que rea-

nori egin dion, jakinarazpenak izan dituen ondorioak eta ezarri diren neurri zuzentzaileak.

45. artikulua.– Sarbide-kontrola.

45.1.– Erabiltzaileek beren zereginak betetzeko behar dituzten datuak eta baliabideak baino ez dituzte atzituko.

45.2.– Fitxategi edo tratamenduaren pertsona erantzuleak izango du ardura, erabiltzaileen eta erabiltzaile-profilen zerrenda eguneratu bat egon dadin (horiek dituzten baimendutako atzipenak adieraziko dituen zerrenda).

45.3.– Fitxategi edo tratamenduaren pertsona erantzuleak mekanismoak ezarriko ditu, erabiltzaile batek baimendu gabeko eskubideak ematen dituzten baliabideak atzitzerik izan ez dezan.

45.4.– Segurtasun-agirian berariaz horretarako baimena duten langileek baino ez dute izango baliabideei buruzko atzipen-baimena eman, aldatu edo kentzeko ahalmena, betiere fitxategi edo tratamenduaren pertsona erantzuleak ezarritako jarraibideen arabera.

45.5.– Fitxategi edo tratamenduaren pertsona erantzulearen mendekoak izan gabe baliabideak atzitu ahal dituzten langileek langile propioek dituzten segurtasunaren inguruko baldintza eta betebehar berberak bete beharko dituzte.

46. artikulua.– Euskarrien eta dokumentuen gestioa.

46.1.– Datu pertsonalak jasota dituzten euskarri eta dokumentuek beti eman behar dute aukera gordetzen duten informazio-mota identifikatu eta datuak inbentarioan jaso ahal izateko; era berean, euskarri eta dokumentu horiek segurtasun-agiriaren arabera baimena duten langileek baino ezingo dituzte atzitu.

Euskarriaren ezaugarri fisikoak direla eta, betebehar hori betetzetik salbuetsi ahalko da, eta salbuespena bera eta salbuespena egiteko arrazoiak idatziz jasoko dira segurtasun-agirian.

46.2.– Datu pertsonalak jasota dituzten euskarri eta dokumentuak (baita posta elektronikoak ere, datu pertsonalak postan bertan edo hari erantsita badituzte) fitxategi edo tratamenduaren pertsona erantzulearen kontrolpean dauden lokaletatik kanpora atera ahal izateko baimena fitxategi edo tratamenduaren pertsona erantzuleak baino ez du emango, eta baimen hori segurtasun-agirian behar bezala jasota egon beharko da.

46.3.– Dokumentazioa lekualdatzean beharrezko neurriak hartuko dira, informazioa garraiatu bitartean inork informazioa hori ostu, galdu edo atzitzerik izan ez dezan.

46.4.– Datu pertsonalak dituzten dokumentu eta euskarriak baztertu behar badira, suntsitu edo ezabatu egingo dira, horietan dagoen informazioa atzitu edo berreskuratzea galarazteko neurriak hartuz.

liza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Artículo 45.– Control de acceso.

45.1.– Las usuarias o usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

45.2.– La persona Responsable del fichero o tratamiento se encargará de que exista una relación actualizada de usuarias o usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

45.3.– La persona Responsable del fichero o tratamiento establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

45.4.– Exclusivamente el personal autorizado para ello en el Documento de Seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por la persona Responsable del fichero o tratamiento.

45.5.– En caso de que exista personal ajeno a la persona Responsable del fichero o tratamiento que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Artículo 46.– Gestión de soportes y documentos.

46.1.– Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el Documento de Seguridad.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el Documento de Seguridad.

46.2.– La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control de la persona Responsable del fichero o tratamiento deberá ser autorizada por la persona Responsable del fichero o tratamiento encontrarse debidamente autorizada en el Documento de Seguridad.

46.3.– En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

46.4.– Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

47. artikulua.– Identifikazioa eta autentifikazioa.

47.1.– Fitxategi edo tratamenduaren pertsona erantzuleak erabiltzaileak modu egokian identifikatu eta autentifikatzeko neurriak hartuko ditu. Horretarako, besteak beste, ziurtagiri digital elektronikoetan edo datu biometrikoen identifikazioan oinarrituriko mekanismoak erabili ahal izango dira.

47.2.– Fitxategi edo tratamenduaren pertsona erantzuleak ezarriko du informazio-sistema atzitzen saiatzen den erabiltzailea zalantzarik gabe eta modu pertsonalizatuan identifikatzeko mekanismoa; aldi berean, mekanismo horrek erabiltzaileak baimena duela egiaztatu beharko du.

47.3.– Autentifikazio-mekanismoa pasahitzetan oinarritzen denean, pasahitzak esleitu, banatu eta gordetzeko prozedura egongo da, pasahitz horiek isilpean eta seguru egongo direla bermatzeko.

47.4.– Segurtasun-agiriak pasahitzak zenbatean behin aldatu behar diren ezarriko du; edonola ere, aldizkakotasun hori ez da urtebetekoa baino luzeagoa izango. Pasahitzak, indarrean dauden bitartean, ulertezin egoteko moduan gordeko dira.

48. artikulua.– Segurtasun- eta berreskurapen-kopiak.

48.1.– Jarduteko prozedurak ezarri beharko dira, gutxienez astean behin segurtasun-kopiak egiteko, epe horretan datuak eguneratu ezean.

48.2.– Halaber, datuak berreskuratzeko prozedurak ezarri beharko dira. Prozedura horiek uneoro bermatu beharko dute datuak galdu edo suntsitu zirenean zeuden bezala utziko dituztela berriz ere.

Datu-fitxategi edo datu-tratamendu partzialki automatizatuak galdu edo suntsitu direnetan baino ezingo dira eskuz grabatu datuak, betiere dagoen dokumentazioak aurreko paragrafoan adierazitako helburua lortzeko aukera ematen badu. Bestalde, segurtasun-agirian jaso beharko dira horrelako gertakariak, arrazoiak adieraziz.

48.3.– Fitxategi edo tratamenduaren pertsona erantzuleak sei hilabetez behin egiaztatu beharko du segurtasun- eta berreskurapen-kopiak egiteko prozedurak ongi zehazturik daudela, funtzionamendu egokia dutela, eta zuzen aplikatzen direla.

48.4.– Datu pertsonalak dituzten fitxategiak tratatzen dituzten informazio-sistemak ezarri edo aldatu aurreko probak ez dira benetako datuekin egingo, baldin eta ez bada egiten den tratamenduari dagokion segurtasun-maila ziurtatzen, eta tratamendu hori ez bada segurtasun-agirian jasotzen.

Probak benetako datuekin egitea aurreikusi bada, aldez aurretik segurtasun-kopia bat egin beharko da.

Artículo 47.– Identificación y autenticación.

47.1.– La persona Responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios. Para ello podrán utilizarse entre otros, mecanismos basados en certificados digitales electrónicos o en el reconocimiento de datos biométricos.

47.2.– La persona Responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario o usuaria que intente acceder al sistema de información y la verificación de que está autorizado.

47.3.– Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

47.4.– El Documento de Seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

Artículo 48.– Copias de respaldo y recuperación.

48.1.– Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

48.2.– Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el Documento de Seguridad.

48.3.– La persona Responsable del fichero o tratamiento se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

48.4.– Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el Documento de Seguridad.

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

BIGARREN ATALA
MAILA ERTAINEKO SEGURTASUN NEURRIAK

49. artikulua.– Auditoretza.

49.1.– Maila ertainetik aurrera, gutxienez bi urtean behin derrigor egin beharko da auditoretza, datuei buruzko informazio-sistemak eta datuak tratatu eta gordetzeko instalazioak aztertzeko.

50. artikulua.– Euskarrien eta dokumentuen gestioa.

50.1.– Euskarrien sarrera-erregistrorako sistema bat ezarri beharko da, zuzenean zein zeharka honako argibide hauek emango dituena: euskarri-mota, eguna eta ordua, igorlea, igorpenean bidalitako dokumentu eta euskarrien kopurua, horiek gordetzen duten informazio-mota, igorpen-mota eta euskarria jasotzeaz arduratuko den pertsona (behar bezala baimendutakoa).

50.2.– Halaber, euskarrien irteera-erregistrorako sistema bat ezarri beharko da, zuzenean zein zeharka honako argibide hauek emango dituena: euskarri-mota, eguna eta ordua, igorlea, igorpenean bidalitako dokumentu eta euskarrien kopurua, horiek gordetzen duten informazio-mota, igorpen-mota eta euskarria igortzeaz arduratuko den pertsona (behar bezala baimendutakoa).

51. artikulua.– Identifikazioa eta autentifikazioa.

Fitxategi edo tratamenduaren pertsona erantzuleak mekanismo bat ezarriko du, informazio-sistema baimenik gabe atzitzeko behin eta berriz egiten diren saiakerak mugatzeko.

52. artikulua.– Sarbide fisikoaren kontrola.

Segurtasun-agiriaren arabera baimena duten langileak baino ezingo dira sartu informazio-sistemari euskarria ematen dioten ekipo fisikoak instalaturik dauden tokietara.

53. artikulua.– Gorabeheren erregistroa.

53.1.– 40. artikuluan araututako erregistroan datuak berreskuratzeko prozedurak ere jaso behar dira, honako hauek adieraziz: prozedura burutu duen pertsona, berreskuratutako datuak, eta berreskurapen-prozeduran eskuz grabatu behar izan diren datuak (datuak eskuz grabatzeko beharrik izan bada).

53.2.– Fitxategi edo tratamenduaren pertsona erantzulearen baimena beharrezkoa izango da, datuak berreskuratzeko prozedurak burutzeko.

HIRUGARREN ATALA
GOI-MAILAKO SEGURTASUN NEURRIAK

54. artikulua.– Euskarrien gestioa eta banaketa.

54.1.– Euskarriak edo dokumentuak identifikatzeko etiketatze-sistemak erabiliko dira; sistema horiek ulergarriak eta esanahidunak izango dira euskarri edo dokumentuak atzitzeko baimena duten erabiltzaileentzat,

SECCIÓN SEGUNDA
MEDIDAS DE SEGURIDAD DE NIVEL MEDIO

Artículo 49.– Auditoria.

49.1.– A partir del nivel medio la auditoria, al menos cada dos años, de los sistemas de información e instalaciones de tratamiento y almacenamiento de datos será obligatoria.

Artículo 50.– Gestión de soportes y documentos.

50.1.– Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

50.2.– Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, la persona destinataria, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

Artículo 51.– Identificación y autenticación.

La persona Responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Artículo 52.– Control de acceso físico.

Exclusivamente el personal autorizado en el Documento de Seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

Artículo 53.– Registro de incidencias.

53.1.– En el registro regulado en el artículo 40 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

53.2.– Será necesaria la autorización de la persona Responsable del fichero o tratamiento para la ejecución de los procedimientos de recuperación de los datos.

SECCIÓN TERCERA
MEDIDAS DE SEGURIDAD DE NIVEL ALTO

Artículo 54.– Gestión y distribución de soportes.

54.1.– La identificación de los soportes o documentos se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios o usuarias con acceso autorizado a los citados

horrela euskarri edo dokumentuen edukia identifikatu ahal izan dezaten. Aitzitik, beste batzuei identifikazioa zailduko dieten etiketatze-sistemak izango dira.

54.2.– Datu pertsonalak dituzten euskarriak banatu behar direnean, datu horiek zifratu egin beharko dira; edo, bestela, beste edozein mekanismo erabili beharko da, garraiatu bitartean informazio hori inork ulertu edo manipulatzerik izan ez dezan.

Era berean, gailu eramangarrietako datuak ere zifratu egingo dira, gailu horiek fitxategi edo tratamenduaren pertsona erantzulearen kontrolpeko instalazioetatik kanpo daudenean.

54.3.– Datu pertsonalak gailu eramangarrietan tratatzea ekidin beharko da, datu horiek zifratzeko aukera ematen ez badute. Hala ere, behar beharrezkoa bada, datuak tratatu egingo dira. Segurtasun-agirian horretarako egon diren arrazoiak jasoko dira, eta tratamendua babesik gabeko egoeretan egiteak dituen arriskuak kontuan hartuko dituzten segurtasun-neurriak hartuko dira.

55. artikulua.– Segurtasun- eta berreskurapen-kopiak.

Datuen segurtasun-kopia bat eta datuak berreskuratzeko prozeduren kopia bat gorde beharko dira datu horiek tratatzen dituzten tresna informatikoak dauden lekuaz bestelako tokiren batean, beti Titulu honetan eskatzen diren segurtasun-neurriak betez, edo informazioa osorik gorde eta berreskuratzeko aukera ematen duten elementuak erabiliz, informazioa berreskuratzeko modurik egon dadin.

56. artikulua.– Atzipenen erregistroa.

56.1.– Atzipen bakoitzeko, gutxienez, argibide hauek gordeko dira: erabiltzailearen identifikazioa, atzipena zein egunetan eta zer ordutan egin den, atzitutako fitxategia, atzipen-mota, eta atzipena baimendu ala ukatu egin den.

56.2.– Atzipena baimendutakoa izan bada, beharrezkoa izango da atzitutako erregistroa identifikatzeko aukera emango duen informazioa gordetzea.

56.3.– Atzipenak erregistratzeko aukera ematen duten mekanismoak horretarako eskumena duen segurtasun-arduradunak kontrolatuko ditu zuzenean; hau da, Segurtasun Informatikorako eta Dokumentuen Gestiorako Batzordeak. Mekanismo horiek inola ere ez dira desaktibatu edo manipulatuko.

56.4.– Erregistroan jasotako datuak gordetzeko epea, gutxienez, bi urtekoa izango da.

56.5.– DBLO segurtasun-arduradunak, Segurtasun Informatikorako eta Dokumentuen Gestiorako Batzordearekin batera, erregistroan jasotako kontrolerako informazioa aztertuko du gutxienez hilabetean behin, eta egindako azterketen eta aurkitutako arazoen inguruko txostena egingo du.

soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

54.2.– La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control de la persona Responsable del fichero o tratamiento.

54.3.– Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el Documento de Seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

Artículo 55.– Copias de respaldo y recuperación.

Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este Título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Artículo 56.– Registro de accesos.

56.1.– De cada intento de acceso se guardarán, como mínimo, la identificación del usuario o usuaria, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

56.2.– En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

56.3.– Los mecanismos que permiten el registro de accesos estarán bajo el control directo del «responsable de seguridad» competente, es decir, el Comité de Seguridad Informática y Gestión Documental, sin que deban permitir la desactivación ni la manipulación de los mismos.

56.4.– El período mínimo de conservación de los datos registrados será de dos años.

56.5.– La persona Responsable de Seguridad LOPD, junto con el Comité de Seguridad Informática y Gestión Documental, se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

56.6.– Artikulu honetan zehaztutako moduan atzipenak erregistratzea ez da beharrezkoa izango, honako kasu hauetan:

a) Fitxategi edo tratamenduaren erantzulea pertsona fisikoa denean.

b) Fitxategi edo tratamenduaren pertsona erantzuleak bermatzen duenean datu pertsonalak berak baino ezin dituela atzitu eta tratatu.

Aurreko puntuan adierazitako kasu horiek berariaz adierazi beharko dira segurtasun-agirian.

57. artikulua.– Telekomunikazioak.

Sare publikoen bidezko edo haririk gabeko sareen bidezko komunikazio elektronikoen bitartez datu pertsonalak transmititzeko, datu horiek zifratu egingo dira; edo, bestela, beste edozein mekanismo erabili beharko da, informazio hori beste inork ulertzeko edo manipulatzeko modurik izan ez dezan.

4. KAPITULUA
DATU-FITXATEGI ETA DATU-TRATAMENDU EZ-AUTOMATIZATUEI EZAR DAKIZKIEKEEN SEGURTASUN-NEURRIAK

LEHENENGO ATALA
OINARRIZKO SEGURTASUN NEURRIAK

58. artikulu.– Guztien betebeharrak.

58.1.– Kapitulu honetan agindutakoaz gain, titulu honetako I. eta II. Kapituluetan xedatutakoa ezarriko zaie fitxategi ez-automatizatuei, honako hauei dagokienez:

a) Garrantzia.

b) Segurtasun-mailak.

c) Tratamenduaren arduraduna.

d) Zerbitzuak datu pertsonalak atzitu gabe ematea.

e) Baimenen eskuordetzea.

f) Fitxategi edo tratamenduaren pertsona erantzulearen eta tratamenduaren arduradunaren lokalez kanpoko lan-araudia.

g) Aldi baterako lanetarako dokumentuen kopiak.

h) Segurtasun-agiria.

58.2.– Halaber, titulu honetako III. Kapituluaren lehenengo atalean ezarritakoa aplikatuko zaie, honako hauei dagokienez:

a) Langileen eginkizunak eta betebeharrak.

b) Segurtasun-gorabeheren erregistroa.

c) Sarbide-kontrola.

d) Euskarrien gestioa.

59. artikulua.– Artxibatzeko irizpideak.

56.6.– No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

a) Que la persona Responsable del fichero o del tratamiento sea una persona física.

b) Que la persona Responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos de carácter personal.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el Documento de Seguridad.

Artículo 57.– Telecomunicaciones.

La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

CAPÍTULO 4
MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS Y TRATAMIENTOS NO AUTOMATIZADOS

SECCIÓN PRIMERA
MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO

Artículo 58.– Obligaciones comunes.

58.1.– Además de lo dispuesto en el presente Capítulo, a los ficheros no automatizados les será de aplicación lo dispuesto en los Capítulos I y II del presente Título en lo relativo a:

a) Alcance.

b) Niveles de seguridad.

c) Encargado o encargada del tratamiento.

d) Prestaciones de servicios sin acceso a datos de carácter personal.

e) Delegación de autorizaciones.

f) Régimen de trabajo fuera de los locales de la persona Responsable del fichero o tratamiento o Encargado del tratamiento.

g) Copias de trabajo de documentos.

h) Documento de Seguridad.

58.2.– Asimismo se les aplicará lo establecido por la Sección Primera del Capítulo III del presente Título en lo relativo a:

a) Funciones y obligaciones del personal.

b) Registro de incidencias.

c) Control de acceso.

d) Gestión de soportes.

Artículo 59.– Criterios de archivo.

Euskarri eta dokumentuak artxibatzeko, dagokion unibertsitateko araudi aplikagarrian ezarritako irizpideak jarraituko dira. Irizpide horiek bermatu beharko dute dokumentuen kontserbazio egokia eta informazioaren lokalizazioa eta kontsulta. Era berean, datuak atzitu, zuzendu, ezereztu eta datuen aurka egiteko eskubideak baliatzeko aukera eman beharko dute.

Arau aplikagarririk ez dagoen kasuetan, fitxategi edo tratamenduaren pertsona erantzuleak ezarriko ditu artxibatzeko jarraitu behar diren irizpideak eta jarduteko prozedurak.

60. artikulua.– Informazioa biltzeko gailuak.

Datu pertsonalak dituzten dokumentuak biltzeko gailuek dokumentu horiek irekitzea galaraziko duten mekanismoak izan beharko dituzte. Dokumentuen ezaugarri fisikoek horretarako aukerarik ematen ez badute, fitxategi edo tratamenduaren pertsona erantzuleak hartuko ditu baimenik ez dutenei atzipena galarazteko neurriak.

61. artikulua.– Euskarrien zaintza.

Datu pertsonalak dituen dokumentazioa aurreko artikuluan ezarri bezala dagokion gailuan bilduta ez badago, dokumentazio hori artxibatu aurreko edo ondorengo azterketa- edo tramitazio-prozesuan dagoelako, horren ardura daukanak zaindu beharko du dokumentazioa, eta uneoro galarazi beharko die atzipena baimenik ez dutenei.

BIGARREN ATALA
MAILA ERTAINEKO SEGURTASUN NEURRIAK

62. artikulua.– Auditoretza.

Maila ertainetik aurrera, fitxategien barne- eta kanpo-auditoretza derrigor egin beharko da gutxienez bi urtetik behin.

HIRUGARREN ATALA
GOI-MAILAKO SEGURTASUN NEURRIAK

63. artikulua.– Informazioa biltegiratzea.

63.1.– Goi-mailako segurtasun-neurriak dituzten datu-fitxategi ez-automatizatuak gordetzeko armairu, agiritegi edo bestelako elementuak egongo dira giltzarekin edo bestelako gailu baliokideren batekin irekitzen diren ateen bidez babesturiko guneetan. Gune horiek itxita egongo dira fitxategiko dokumentuak atzitzeko beharrik ez dagoenean.

63.2.– Fitxategi edo tratamenduaren pertsona erantzuleak dituen lokalen ezaugarriak direla-eta ezin bada bete aurreko puntuan ezarritakoa, pertsona erantzuleak bestelako neurriak hartuko ditu. Segurtasun-agirian adieraziko da zer neurri hartu diren eta zergatik.

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en la respectiva normativa universitaria aplicable. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

En aquellos casos en los que no exista norma aplicable, la persona Responsable del fichero o tratamiento deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

Artículo 60.– Dispositivos de almacenamiento.

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, la persona Responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Artículo 61.– Custodia de los soportes.

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecido en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

SECCIÓN SEGUNDA
MEDIDAS DE SEGURIDAD DE NIVEL MEDIO

Artículo 62.– Auditoria.

A partir del nivel medio la auditoria interna o externa de los ficheros, al menos cada dos años, será obligatoria.

SECCIÓN TERCERA
MEDIDAS DE SEGURIDAD DE NIVEL ALTO

Artículo 63.– Almacenamiento de la información.

63.1.– Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal de nivel alto deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

63.2.– Si, atendidas las características de los locales de que dispusiera la persona Responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, la persona responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el Documento de Seguridad.

64. artikulua.– Kopia edo erreprodukzioa.

64.1.– Kopiak egin edo dokumentuak erreproduzituko dira segurtasun-agiriaren arabera horiek kontrolatzeko baimena duen pertsonaren kontrolpean, ez bestela.

64.2.– Baztertutako kopiak edo erreprodukzioak suntsitu egin beharko dira, inork bertako informazioa atzitu edo geroago berreskuratzerik izan ez dezan.

65. artikulua.– Dokumentazioa atzitzea.

65.1.– Baimena dutenek baino ezingo dute atzitu dokumentazioa.

65.2.– Erabiltzaile askok erabil ditzaketen dokumentuen kasuan, egin diren atzipenak identifikatzeko mekanismoak ezarriko dira.

65.3.– Aurreko paragrafoan aipatutakoak ez diren pertsonek egindako atzipenak behar bezala erregistratuko dira, horretarako segurtasun-agirian ezarritako prozedurarekin bat etorriz.

66. artikulua.– Dokumentazioa lekualdatzea.

Fitxategi bateko dokumentazioa fisikoki lekualdatu behar denean, lekualdatzen den informazioa atzitu edo manipulatzea galarazteko neurriak hartuko dira.

VI. TITULUA

DATUAK BABESTEKO EUSKAL BULEGOA

67. artikulua.– Datuak Babesteko Euskal Bulegoa.

67.1.– Otsailaren 25eko 2/2004 Legeak, datu pertsonaletarako jabetza publikoko fitxategiei eta Datuak Babesteko Euskal Bulegoa sortzeari buruzkoak, ezartzen du bulego hori zuzenbide publikoko entea izango dela, nortasun juridiko propioa eta gaitasun publiko eta pribatu erabatekoa izango dituela, eta herri-administrazioekiko inongo loturarik gabe beteko dituela bere eginkizunak.

67.2.– Datuak Babesteko Euskal Bulegoak herritarren intimitate pertsonala eta etxekoena babesteko eginbeharra hartzen du bere gain, baita herritarrek legeak onartzen dizkien eskubideak baliatzeko duten ahala zaintzekoa ere, datuak babesteari buruzko araudia betetzeko ardura hartuz. Kontrol-agintaritza moduan jarduten du eginkizun horiek betetzeko, eta horretarako lanerako erabateko objektibitatea eta independentzia bermatzen dizkio legeak.

67.3.– Datuak Babesteko Euskal Bulegoaren kontrol-eremuaren barruan dago UPV/EHU.

68. artikulua.– Datuak Babesteko Euskal Bulegoaren jarduerak.

Artículo 64.– Copia o reproducción.

64.1.– La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el Documento de Seguridad.

64.2.– Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Artículo 65.– Acceso a la documentación.

65.1.– El acceso a la documentación se limitará exclusivamente al personal autorizado.

65.2.– Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos, que puedan ser utilizados por múltiples usuarios o usuarias.

65.3.– El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el Documento de Seguridad.

Artículo 66.– Traslado de documentación.

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

TÍTULO VI

LA AGENCIA VASCA DE PROTECCIÓN DE DATOS

Artículo 67.– La Agencia Vasca de Protección de Datos.

67.1.– La Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos, configura a ésta como ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las administraciones públicas en el ejercicio de sus funciones.

67.2.– La Agencia Vasca de Protección de Datos asume como misión proteger la intimidad personal y familiar de los ciudadanos o ciudadanas y el legítimo ejercicio de sus derechos, velando por el cumplimiento de la normativa sobre protección de datos de carácter personal. En el ejercicio de su actividad, tiene la consideración de autoridad de control y la ley le garantiza la plena independencia y objetividad en el ejercicio de su cometido.

67.3.– Entre las entidades públicas que están dentro del ámbito de control de la Agencia Vasca de Protección de Datos se encuentra la UPV/EHU.

Artículo 68.– Actividades de la Agencia Vasca de Protección de Datos.

Datuak Babesteko Euskal Bulegoak, legeak ematen dizkion funtzioak betetzeko, besteak beste, honako lan edo jarduera hauek egiten ditu:

a) Datu pertsonalen tratamenduaren inguruan dituzten eskubideei buruzko informazioa ematen die pertsonei; era berean, laguntza eta babesa eskaintzen die, eskubide horiek balia ditzaten.

b) Legezkoak ez diren jokabideak aztertzen ditu, eta hala badagokio, egin diren arau-hausteei buruzko erabakiak hartu eta beharrezko neurriak hartzen ditu, datuen tratamendua indarrean dagoen legediarekin bat etor dadin.

c) Datu pertsonalak dituzten fitxategien erregistroa gordetzen du. Bertan Euskal Autonomia Erkidegoko administrazio publikoek eta zuzenbide publikoko erakundeek beren fitxategiak erregistratu beharko dituzte, beren eginkizunak betetzeko fitxategi horietan nolako datu pertsonalak tratatu eta biltzen dituzten adieraziz.

d) Datu pertsonalak babesteari dagokionez pertsonek nahiz erakundeek egindako kontsulta eta txostenenez arduratzen da.

e) Datuak babesteari buruzko kultura hedatu eta zabaltzen du, alde batetik, gizarteko taldeak sentsibilizatuz; eta, beste alde batetik, erakunde publikoetako langileak prestatuz, jardunbide hobeak har ditzaten.

XEDAPEN IRAGANKORRA

Arautegi honetako V. Tituluan jasotako segurtasun-neurriek UPV/EHUrentzat duten izaera loteslea egokituko da DBLOGEk segurtasun-neurrien derrigortasunari buruz bigarren xedapen iragankorrean ezartzen duenera.

AZKEN XEDAPENA.– Arautegia eta eranskinak eguneratzea - Indarrean sartzea

Aldian behin arautegi hau berrikusi egingo da, izan daitezkeen arauzko eskakizun berrien arabera, edo aurkitzen diren arautu beharreko suposamenduen arabera.

Eranskinak aldatu edo gehitzeko erabakiak hartu ahal izango dira UPV/EHUko Zuzendaritza Kontseiluko kideen botoen gehiengoarekin eta Idazkaritza Nagusiaren eta Gerentziaren baterako proposamenarekin.

Datuak Babesteko Batzordeak Idazkaritza Nagusiari igorri ahalko dizkio bere aldaketa-proposamenak.

Arautegiaren bertsio eguneratua unibertsitatearen web-orrian egongo da eskuragarri (www.ehu.es/babestu).

Arautegi hau indarrean jarriko da 2008ko urriaren 1ean, Datuak Babesteko Euskal Bulegoan behar bezala erregistratu ondoren.

Para el ejercicio de las funciones que la ley confiere a la Agencia Vasca de Protección de Datos, ésta desempeña, entre otras, las siguientes tareas o actividades:

a) Informar a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal y ayudarles y tutelarles en el ejercicio de los mismos.

b) Investigar aquellas actuaciones contrarias a la ley y resolver, en su caso, sobre las infracciones producidas y requerir la adopción de las medidas necesarias para la adecuación del tratamiento de datos a la legislación en vigor.

c) Mantener un Registro de Ficheros de Datos de Carácter Personal, en el cual las administraciones públicas y entes de derecho público de la Comunidad Autónoma del País Vasco han de inscribir sus ficheros, declarando los tipos de datos de carácter personal que recogen y tratan para el cumplimiento de sus fines.

d) Atender todo tipo de consultas e informes que, en relación a la protección de datos, le sean solicitados por personas e instituciones.

e) Difundir y extender la cultura de la protección de datos, sensibilizando a los colectivos sociales y potenciando la formación y la adopción de mejores prácticas por parte de los trabajadores de las instituciones públicas.

DISPOSICIÓN TRANSITORIA

El carácter vinculante para la UPV/EHU de las medidas de seguridad previstas en el Título V del presente Reglamento, se ajustará a lo establecido en la Disposición Transitoria Segunda del RDLOPD en relación con la obligatoriedad de las medidas de seguridad exigidas por dicho RDLOPD.

DISPOSICIÓN FINAL.– Actualización del Reglamento y de los anexos - Entrada en vigor.

Este Reglamento será periódicamente actualizado en función de los nuevos requisitos normativos que puedan ser exigidos y los supuestos susceptibles de regulación que se vayan detectando.

Las modificaciones e incorporaciones de anexos podrán ser realizadas mediante acuerdo adoptado por la mayoría de los miembros del Consejo de Dirección de la UPV/EHU, a propuesta conjunta de la Secretaría General y la Gerencia.

La Comisión para la Protección de Datos podrá enviar a la Secretaría General sus propuestas de cambio.

La versión actualizada del Reglamento estará disponible en la página web de la Universidad (www.ehu.es/babestu).

El presente Reglamento entrará en vigor el 1 de octubre de 2008, una vez de haber sido debidamente registrado en la Agencia Vasca de Protección de Datos.

I. EREDUEI BURUZKO ERANSKINAK ETA INFORMAZIO OSAGARRIA

I.I.E. DOKUMENTU EDO PANTAILETAKO INFORMAZIO-KLAUSULAREN EREDUA

Datu Pertsonalak Babesteari buruzko abenduaren 13ko 15/1999 Lege Organikoari jarraiki, adierazten dizugu zure datuak UPV/EHUren _____ fitxategian sartuko ditugula. Fitxategi horren helburua da _____ _____

Jakinarazten dizugu datuak atzitu, zuzendu, ezereztu edo datuen aurka egiteko eskubideak balia ditzakezula. Horretarako, idazki bat igorri behar diozu UPV/EHUko DBLO segurtasun-arduradunari helbide honetara:UPV/EHU - Errektoregoa - Sarriena auzoa, z.g. 48940 Leioa (Bizkaia). Idazkiari zure identitatea egiaztatzeko dokumentuaren kopia erantsi behar diozu.

Datu Pertsonalak Babesteari buruzko UPV/EHUren arautegia kontsulta dezakezu interneteko helbide honetan: www.ehu.es/babestu.

I. ANEXOS RELATIVOS A MODELOS E INFORMACIÓN COMPLEMENTARIA

I.M.I CLÁUSULA INFORMATIVA TIPO EN DOCUMENTOS Y/O PANTALLAS

De acuerdo con lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, le informamos que sus datos pasan a formar parte del fichero _____ de la UPV/EHU, cuya finalidad es_____ _____.

Le comunicamos que puede ejercitar los derechos de acceso, rectificación, cancelación y oposición de sus datos remitiendo un escrito a la persona Responsable de Seguridad LOPD de la UPV/EHU, Rectorado, Barrio Sarriena s/n, 48940 Leioa - Bizkaia, adjuntando copia de documento que acredite su identidad.

Puede consultar el «Reglamento de la UPV/EHU para la Protección de Datos de carácter Personal» en las direcciones de Internet www.ehu.es/babestu.

ERANSKINA

I.II.E. DATU-TRATAMENDUAREKIKO ADOSTASUNA EZEZTATZEA

UPV/EHURI NIRE DATU PERTSONALAK TRATATZEAREKIKO AGERTUTAKO ADOSTASUNA EZEZTATZEKO ESKAERA

Nire datu pertsonalak tratatzearekiko adostasuna ezeztatzeak ukitzen d(it)uen fitxategi(ar)ei buruzko datuak:

Fitxategi(ar)en izena(k)							
Tratamenduaren deskribapena							
Adostasuna zein egunetan eman zen							
Nori zuzendua	EUSKAL HERRIKO UNIBERTSITATEA Informazio eta Komunikazio Teknologietarako Gerenteordetza Nori zuzendua: DBLO segurtasun-arduraduna						
Auzoa	Sarriena			Zk.	-	Solairua	-
Herria	Leioa	Lurralde historikoa	Bizkaia		Posta-kodea	48940	

Eskatzaileari buruzko datuak:

Abizenak							
Izena		NAN					
Kalea				Zk.		Solairua	
Herria		Lurralde historikoa			Posta-kodea		
Telefonoa		Posta elektronikoa					

Legezko ordezkariari buruzko datuak:

Abizenak			
Izena		NAN	

ESKATZEN DUT:

1.– UPV/EHUri nire datu pertsonalak tratatzearekiko agertutako adostasuna ezeztatzea.
2.– Adostasuna benetan ezeztatu dela niri jakinaraztea.
3.– Nire datuen jakinarazpena jaso duten fitxategi edo tratamenduen pertsona erantzuleei jakinaraztea adostasuna ezeztatu dela.

Tokia eta eguna	
Eskatzailearen sinadura	

ANEXO

I.M.II REVOCACIÓN DEL CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS

SOLICITUD DE REVOCACIÓN DE CONSENTIMIENTO OTORGADO PARA EL TRATAMIENTO DE MIS DATOS DE CARÁCTER PERSONAL POR PARTE DE LA UPV/EHU

Datos del fichero/s en el/los que solicito la revocación de mi consentimiento al tratamiento de mis datos de carácter personal:

Nombre del fichero/s						
Descripción del tratamiento						
Fecha del Consentimiento						
Dirigido a	*UNIVERSIDAD Del PAÍS VASCO / EUSKAL HERRIKO UNIBERTSITATEA* *Vicegerencia de las Tecnologías de la Información y las Comunicaciones* *A la atención de: Responsable de Seguridad LOPD*					
Barrio	*Sarriena*			*N.º*	-	*Piso* -
Localidad	*Leioa*	*Terr. Histórico*	*Bizkaia*		*Cód. Postal*	*48940*

Datos del o de la solicitante:

Apellidos					
Nombre		*DNI*			
Calle			*N.º*	*Piso*	
Localidad		*Terr. Histórico*		*Cód. Postal*	
Telefono		*Correo electrónico*			

Datos del o de la representante legal:

Apellidos			
Nombre		*DNI*	

SOLICITO:

1.– La revocación del consentimiento dado para el tratamiento arriba descrito por parte de la UPV/EHU.
2.– Notificarme la materialización de la revocación de consentimiento planteada.
3.– Notificar a las personas responsables de ficheros o tratamientos a quiénes hubieran sido comunicados los datos la revocación del consentimiento practicada.

Lugar y fecha	
Firma del o de la solicitante	

INFORMAZIO OSAGARRIA

I.– Formularioa betetzeko eta idazkiari dokumentazioa eransteko argibideak:

• Formularioaren atal guztiak bete behar dira, eta formulario hori interesdunak izenpetu beharko du.

• Beti aurkeztu behar da NANaren fotokopia edo interesduna identifikatuko duen beste edozein dokumentu baliodunena.

• Interesduna adin txikikoa bada edo ezgaiturik badago, bere ordezkari legalaren NANaren fotokopia aurkeztu beharko da, edo ordezkari hori identifikatuko duen beste edozein dokumentu baliodun; baita ordezkaritza legezkoa dela egiaztatzen duen benetako agiriaren fotokopia ere.

II.– Eskubidea baliatzen duenak jarraitu beharreko prozedura:

• Adostasuna ezeztatzeko idazki bat aurkeztu beharko zaio DABLO segurtasun-arduradunari, unibertsitateko erregistro orokorrean edo UPV/EHUko 2007ko maiatzaren 28ko erabakian zerrendatutako bulegoetan (2007ko abuztuaren 3ko EHAA, 149. zk.); bestela, Herri Administrazioen Araubide Juridikoaren eta Administrazio Prozedura Erkidearen azaroaren 26ko 30/1992 Legeko 38.4. artikuluak ezarritako bideak erabiliz ere aurkez daiteke idazkia.

• Idazkia bidali dela frogatze aldera, komeni da UPV/EHUko erregistroko sarrera-zigilua egiaztagiritzat gordetzea.

III.– Fitxategi edo tratamenduaren pertsona erantzuleak jarraitu beharreko prozedura:

• Pertsona erantzuleak gehienez hamar egun balioduneko epea izango du eskatzaileari erantzuteko, bere eskaera jasotzen duen egunetik kontatzen hasita.

• Epe hori amaitu eta atzipen-eskaerari buruzko erantzun garbirik egon ez bada, eskaerari uko egin zaiola ulertuko da.

• Adostasuna ezeztatzeko eskaera baietsi bada, interesdunak jakinarazpena jasotzeko aukeratutako moduan adierazi beharko dio pertsona erantzuleak eskaera baietsi dela, berori jasotzen duen egunetik kontatzen hasi eta hamar egun balioduneko epean.

• Adostasuna ezeztatzeak ez du atzeraeraginezko ondoriorik izango.

• Datuak tratatzeko adostasun-ezeztatzea gauzatzeko ez da ezer ordainduko.

INFORMACIÓN COMPLEMENTARIA

I.– Instrucciones para la cumplimentación del formulario y documentación a aportar junto al escrito:

• Se deberá rellenar la totalidad de los apartados solicitados en el formulario y éste debe ser firmado por la persona interesada.

• En todo caso, será necesario la entrega de la fotocopia de DNI o cualquier otro medio de identificación personal válido en derecho del interesado.

• En el supuesto de que la persona interesada sea menor o esté incapacitada, será necesario la entrega también de la fotocopia de DNI o cualquier otro medio de identificación personal válido en derecho del o de la representante legal, debiéndose además en este caso presentar una fotocopia del documento acreditativo auténtico de la representación legal.

II.– Requisitos del procedimiento para el que ejercita el derecho:

• La revocación del consentimiento se ejercerá mediante escrito dirigido a la persona Responsable de Seguridad LOPD, a través del Registro General de la Universidad en cualquiera de las oficinas enumeradas en la Resolución de la UPV/EHU de 28 de mayo de 2007 (BOPV n.º 149, de 3 de agosto de 2007), o por cualesquiera de los medios previstos en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

• Es aconsejable, desde el punto de vista probatorio, acreditar la remisión del escrito, mediante sello de entrada en el registro de la UPV/EHU.

III.– Requisitos del procedimiento para la persona Responsable del Fichero o tratamiento:

• La persona responsable deberá responder al o a la solicitante en el plazo máximo de diez días hábiles, a contar desde la recepción de la solicitud.

• Transcurrido este plazo sin que de forma expresa se conteste a la petición de acceso, ésta se entenderá denegada.

• Si la solicitud de revocación del consentimiento fuese estimada, la persona responsable deberá informar a la persona interesada, en la forma elegida por éste, en el plazo de diez días hábiles a contar desde la fecha de la recepción de la solicitud.

• A la revocación del consentimiento no se le atribuirán efectos retroactivos.

• La materialización de la revocación del consentimiento al tratamiento de datos es gratuita.

IV.– Araudi aplikagarria:

• Datu Pertsonalak Babesteari buruzko 15/1999 Lege Organikoa, abenduaren 13koa, 6.3 artikulua.

• Abenduaren 21eko 1720/2007 Errege Dekretua, Datu Pertsonalak Babesteari buruzko abenduaren 13ko 15/1999 Lege Organikoa garatuko duen erregelamendua onartzen duena, 17. artikulua.

• Datu Pertsonalak Babesteari buruzko UPV/EHUren Arautegia, unibertsitateko Gobernu Kontseiluak 2008ko apirilaren 10ean onartua, 11.5. artikulua.

V.– Erreklamazioak (eskubideen babesa):

• Eskatzaileak uste badu oztopoak jarri zaizkiola bere datuak tratatzearekiko agertutako adostasuna ezeztatzeko eskubidea baliatu ahal izateko, erreklamazioa egin dezake Datuak Babesteko Euskal Bulegoan, bertan bere eskubideak babesteko prozedura abiaraz dezaten.

• Hori egin aurretik, bere datuak tratatzearekiko adostasuna ezeztatzeko eskubidea baliatu ahal izateko eskaera egiten duen egunetik hamar egun igaro beharko dira, bitarte horretan erantzun garbirik jaso gabe.

• Erreklamazioa Datuak Babesteko Euskal Bulegoari zuzenduko zaio (Tomas Zumarraga Dohatsuaren kalea 71, 3a - 01008 Vitoria-Gasteiz - Tel. 945 01 62 30 - Faxa: 945 01 62 31, avpd@avpd.es), eta agiri hauek aurkeztuko dira:

– Adostasun-ezeztatzea gauzatzeari DBLO segurtasun-arduradunak egindako ukoa.

– Adostasuna ezeztatzeko ereduaren kopia, UPV/EHUren erregistroko sarrera-zigiluarekin.

– Posta-bulegoko zigiluaren kopia, eskaera ohiko postaz egin bada.

IV.– Normativa de aplicación:

• Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, artículo 6.3.

• Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, artículo 17.

• Reglamento de la UPV/EHU para la protección de datos de carácter personal, aprobado por el Consejo de Gobierno de la Universidad de 10 de abril de 2008, artículo 11.5.

V.– Reclamaciones (Tutela de derechos):

• Si el o la solicitante entiende que no se le ha facilitado correctamente el derecho de revocación del consentimiento otorgado para el tratamiento de sus propios datos, puede reclamar ante la Agencia Vasca de Protección de Datos para que inicie un procedimiento de tutela de sus derechos.

• Para ello, resulta necesario que haya transcurrido el plazo de diez días desde la solicitud del derecho de revocación del consentimiento para el tratamiento de sus propios datos, sin que de forma expresa se le haya contestado.

• La reclamación se dirigirá a la Agencia Vasca de Protección de Datos (c/ Beato Tomás de Zumárraga, 71, 3.º - 01008 Vitoria-Gasteiz - Tel. 945 01 62 30 - Fax. 945 01 62 31 avpd@avpd.es - www.avpd.es), aportándose alguno de los siguientes documentos:

– La negativa de la persona Responsable de Seguridad LOPD a llevar a cabo la revocación del consentimiento.

– Copia del modelo de revocación del consentimiento, sellada por el registro de entrada de la UPV/EHU.

– Copia del sello de la oficina de correos si la solicitud se ha remitido por correo ordinario.

ERANSKINA

I.III.E. DATUAK TRATATZEKO BAIMENA EMATEA.

INTERESDUNARI BURUZKO DATUAK

Adinez nagusia den .... jaunak/andreak, ... kaleko .....zenbakian, ... posta-kodea duen ..... herrian, ... probintzian bizi denak, eta . ..... zenbakidun NANaren kopia eransten duenak, idazki honen bidez:

«Bere datu pertsonalak tratatzeko baimena ematen du, eta datu horiek [dagokion helburua adierazi]tzeko helburua duen UPV/EHUren [dagokion fitxategia adierazi] fitxategian sartzekoa ere bai, bat etorriz 2007ko apirilaren 11ko EHAAn (69. zk.) argitaratu zen fitxategiei buruzko UPV/EHUren ebazpenean ezarritakoarekin.»

Datu Pertsonalak Babesteari buruzko abenduaren 13ko 15/1999 Lege Organikoarekin bat etorriz, eta unibertsitateko Gobernu Kontseiluak apirilaren 10ean onartutako Datu Pertsonalak Babesteari buruzko UPV/EHUren Arautegian ezarritakoaren arabera, interesdunak eskubidea izango du datuak atzitu, zuzendu, ezereztu edo datuen aurka egiteko eskubideak baliatzeko. Horretarako, idazki bat igorri behar dio UPV/EHUko DBLO segurtasun-arduradunari helbide honetara:UPV/EHU - Errektoregoa - Sarriena auzoa, z.g. 48940 Leioa (Bizkaia). Idazkiari bere identitatea egiaztatzeko dokumentuaren kopia erantsi behar dio.

Interesdunaren sinadura:

OHARRA:

* Interesdunaren ideologia, erlijio edo sinesmenari buruzko datuak bilduko balira, interesdunari datu horiek tratatzeko debekua ezar dezakeela jakinaraziko zaio.

ANEXO

I.M.III CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS

DATOS DE LA PERSONA INTERESADA

D./D.ª …..... ....., mayor de edad, con domicilio en la c/ …..... ..... n.º …....., Localidad …....., Provincia …..... ..... Código Postal …..... con DNI …....., del que se acompaña fotocopia, por medio del presente escrito manifiesta que:

«Por la presente autoriza el tratamiento de sus datos de carácter personal y su inclusión en el fichero de [introducir fichero correspondiente] de la UPV/EHU, cuya finalidad es [introducir la finalidad del fichero correspondiente], de acuerdo con lo dispuesto en la Declaración de ficheros de la UPV/EHU publicada de el BOPV n.º 69, de 11 de abril de 2007.»

De conformidad con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal y en función de lo establecido en el Reglamento de la UPV/EHU para la protección de datos de carácter personal, aprobado por el Consejo de Gobierno de la Universidad de fecha 10 de abril de 2008, la persona interesada tendrá la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, mediante escrito dirigido a la persona Responsable de Seguridad LOPD de la UPV/EHU, Rectorado, Barrio Sarriena s/n, 48940 Leioa - Bizkaia, adjuntando copia de documento que acredite su identidad.

Firma de la persona interesada:

ADVERTENCIA:

* En el caso de que se recabasen datos relativos a la ideología, religión o creencias de la persona interesada, éste deberá ser advertido de su derecho a no consentir el tratamiento de tales datos.

ERANSKINA

I.IV.E. ATZIPEN-ESKUBIDEA

UPV/EHUREN FITXATEGIETAKO NIRE DATU PERTSONALAK ATZITZEKO ESKAERA

Nire datu pertsonalak atzitzeko eskaerak ukitzen d(it)uen fitxategi(ar)ei buruzko datuak:

Fitxategi(ar)en izena(k)						
Nori zuzendua	EUSKAL HERRIKO UNIBERTSITATEA Informazio eta Komunikazio Teknologietarako Gerenteordetza Nori zuzendua: DBLO segurtasun-arduraduna					
Auzoa	Sarriena		Zk.	-	Solairua	-
Herria	Leioa	Lurralde historikoa	Bizkaia		Posta-kodea	48940

Eskatzaileari buruzko datuak:

Abizenak						
Izena		NAN				
Kalea			Zk.		Solairua	
Herria		Lurralde historikoa			Posta-kodea	
Telefonoa		Posta elektronikoa				

Legezko ordezkariari buruzko datuak:

Abizenak			
Izena		NAN	

Datu pertsonalak babesteari buruzko arautegian ezarritakoarekin bat etorriz, atzipen-eskubidea baliatu nahi dut; beraz, ESKATZEN DUT adierazitako fitxategia(k) atzitzeko doako aukera izatea, bertan dauden nire datu pertsonal guztien berri eman diezadaten, eskaera hau jasotzen den egunetik kontatzen hasi eta gehienez hilabete bateko epean. Informazio hori era honetara eman diezadaten nahi dut, betiere horrela egitea posible bada:

☐ Ni neu bertaratu eta pantailan begiratuz.
☐ Posta bidez idazkia, kopia edo fotokopia jasoz adierazitako helbidean.
☐ Posta elektronikoa edo bestelako komunikazio-sistema elektronikoren bat erabiliz.
☐ Fitxategiaren konfigurazioarekin, ezarpen materialarekin edo tratamendu-motarekin bateragarria den beste edozein prozedura jarraituz.

Tokia eta eguna	
Eskatzailearen sinadura	

ANEXO

I.M.IV DERECHO DE ACCESO

SOLICITUD DE EJERCICIO DEL DERECHO DE ACCESO A MIS DATOS DE CARÁCTER PERSONAL INSCRITOS EN FICHERO DE LA UPV/EHU

Datos del fichero/s en el/los que solicito el acceso a mis datos de carácter personal:

Nombre del Fichero/s	
Dirigido a	*UNIVERSIDAD DEL PAÍS VASCO / EUSKAL HERRIKO UNIBERTSITATEA* *Vicegerencia de las Tecnologías de la Información y las Comunicaciones* *A la atención de: Responsable de Seguridad LOPD*

Barrio	*Sarriena*				*N.º*	-	*Piso*	-	
Localidad	*Leioa*	*Terr. Histórico*	*Bizkaia*		*Cód. Postal*	*48940*			

Datos del o de la solicitante:

Apellidos									
Nombre		*DNI*							
Calle					*N.º*		*Piso*		
Localidad		*Terr. Histórico*			*Cód. Postal*				
Telefono		*Correo electrónico*							

Datos del o de la representante legal:

Apellidos			
Nombre		*DNI*	

Deseo ejercer mi derecho de acceso, de conformidad con lo establecido en la normativa sobre protección de datos, por lo que SOLICITO se me facilite gratuitamente el derecho de acceso a el/los fichero/s indicado/s, informándome sobre todos mis datos de carácter personal en él/ellos contenidos, en el plazo máximo de un mes a contar desde la recepción de esta solicitud. Deseo que la información solicitada me sea facilitada, siempre que sea materialmente posible de la siguiente manera:

☐ *Presencialmente mediante visualización en pantalla.*
☐ *Escrito, copia o fotocopia remitida por correo a la dirección indicada.*
☐ *Correo electrónico u otros sistemas de comunicaciones electrónicas.*
☐ *Cualquier otro procedimiento que sea adecuado a la configuración e implantación material del fichero o la naturaleza del tratamiento.*

Lugar y fecha	
Firma del o de la solicitante	

INFORMAZIO OSAGARRIA

I.– Formularioa betetzeko eta idazkiari dokumentazioa eransteko argibideak:

• Formularioaren atal guztiak bete behar dira, eta formulario hori interesdunak izenpetu beharko du.

• Beti aurkeztu behar da NANaren fotokopia edo interesduna identifikatuko duen beste edozein dokumentu baliodunena.

• Interesduna adin txikikoa bada edo ezgaiturik badago, bere ordezkari legalaren NANaren fotokopia aurkeztu beharko da, edo ordezkari hori identifikatuko duen beste edozein dokumentu baliodun; baita ordezkaritza legezkoa dela egiaztatzen duen benetako agiriaren fotokopia ere.

II.– Eskubidea baliatzen duenak jarraitu beharreko prozedura:

• Datuak atzitzeko eskubidea ezingo da baliatu 12 hilabeteko epearen barruan behin baino gehiagotan, interesdunak eskubidea gehiagotan baliatzeko bidezko interesa duela egiaztatu ezean.

• Atzipen-eskubidea baliatzeko idazki bat aurkeztu beharko zaio DBLO segurtasun-arduradunari, unibertsitateko erregistro orokorrean edo UPV/EHUko 2007ko maiatzaren 28ko erabakian zerrendatutako bulegoetan (2007ko abuztuaren 3ko EHAA, 149. zk.); bestela, Herri Administrazioen Araubide Juridikoaren eta Administrazio Prozedura Erkidearen azaroaren 26ko 30/1992 Legeko 38.4. artikuluak ezarritako bideak erabiliz ere aurkez daiteke idazkia.

• Idazkia bidali dela frogatze aldera, komeni da UPV/EHUko erregistroko sarrera-zigilua egiaztagiritzat gordetzea.

III.– Fitxategi edo tratamenduaren pertsona erantzuleak jarraitu beharreko prozedura:

• Pertsona erantzuleak gehienez hilabete bateko epea izango du eskatzaileari erantzuteko, bere eskaera jasotzen duen egunetik kontatzen hasita.

• Epe hori amaitu eta atzipen-eskaerari buruzko erantzun garbirik egon ez bada, eskaerari uko egin zaiola ulertuko da.

• Atzipen-eskubidea baliatzeko eskaera baietsi bada, interesdunak jakinarazpena jasotzeko aukeratutako moduan adierazi beharko dio pertsona erantzuleak eskaera baietsi dela, berori jasotzen duen egunetik kontatzen hasi eta hamar egun balioduneko epean. Interesdunak aukeratu duen kontsultarako bidea alde batera utzita, UPV/EHUk erabaki dezake kontsultarako zer sistema erabili, interesdunak egindako aukerak unibertsitateari zerbitzuak normaltasunez ematea galarazten badio.

INFORMACIÓN COMPLEMENTARIA

I.– Instrucciones para la cumplimentación del formulario y documentación a aportar junto al escrito:

• Se deberá rellenar la totalidad de los apartados solicitados en el formulario y éste debe ser firmado por la persona interesada.

• En todo caso, será necesario la entrega de la fotocopia de DNI o cualquier otro medio de identificación personal válido en derecho de la persona interesada.

• En el supuesto de que la persona interesada sea menor o esté incapacitada, será necesario la entrega también de la fotocopia de DNI o cualquier otro medio de identificación personal válido en derecho del o de la representante legal, debiéndose además en este caso presentar una fotocopia del documento acreditativo auténtico de la representación legal.

II.– Requisitos del procedimiento para el que ejercita el derecho:

• El derecho de acceso no podrá llevarse a cabo en intervalos inferiores a 12 meses, salvo interés legítimo debidamente justificado.

• El derecho de acceso se ejercerá mediante escrito dirigido a la persona Responsable de Seguridad LOPD, a través del Registro General de la Universidad en cualquiera de las oficinas enumeradas en la Resolución de la UPV/EHU de 28 de mayo de 2007 (BOPV n.º 149, de 3 de agosto de 2007), o por cualesquiera de los medios previstos en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

• Es aconsejable, desde el punto de vista probatorio, acreditar la remisión del escrito, mediante sello de entrada en el registro de la UPV/EHU.

III.– Requisitos del procedimiento para la persona Responsable del Fichero o tratamiento:

• La persona responsable deberá responder al o a la solicitante en el plazo máximo de un mes, a contar desde la recepción de la solicitud.

• Transcurrido este plazo sin que de forma expresa se conteste a la petición de acceso, ésta se entenderá denegada.

• Si la solicitud del derecho de acceso fuese estimada, la persona responsable deberá informar a la persona interesada, en la forma elegida por éste, en el plazo de diez días hábiles a contar desde la fecha de la estimación. Al margen de la opción de consulta seleccionada por la persona interesada, la UPV/EHU podrá determinar el sistema de consulta cuando el requerido por la persona interesada perturbe la normal prestación de los servicios de la Universidad.

• Ematen den informazioa ulergarria eta irakurgarria izan beharko da, eta honako hauek zehaztu beharko ditu: interesdunari buruz fitxategian zer datu dauden, eta zer datu sortu diren edozein lanketa, tratamendu edo prozesuren ondorioz; datuek zer jatorri duten eta lagapen-hartzaileak nortzuk diren (lagapen-hartzaileak datuen jakinarazpena jaso duten edo jasoko duten erakunde publiko nahiz pribatuak izango dira); eta datuak zergatik eta zertarako bildu edo gorde ziren.

• Datuak atzitzea doakoa da.

IV.– Araudi aplikagarria:

• Datu Pertsonalak Babesteari buruzko 15/1999 Lege Organikoa, abenduaren 13koa, 15 artikulua.

• Abenduaren 21eko 1720/2007 Errege Dekretua, Datu Pertsonalak Babesteari buruzko abenduaren 13ko 15/1999 Lege Organikoa garatuko duen erregelamendua onartzen duena, 23, 24, 25, 26, 27, 28, 29 eta 30. artikuluak.

• 2/2004 Legea, otsailaren 25ekoa, datu pertsonaletarako jabetza publikoko fitxategiei eta Datuak Babesteko Euskal Bulegoa sortzeari buruzkoa, 8. eta 9. artikuluak.

• 308/2005 Dekretua, urriaren 18koa, datu pertsonaletarako jabetza publikoko fitxategiei eta Datuak Babesteko Euskal Bulegoa sortzeari buruzko otsailaren 25eko 2/2004 Legea garatzen duena, 6, 7, eta 8. artikuluak.

• Datu Pertsonalak Babesteari buruzko UPV/EHUren Arautegia, unibertsitateko Gobernu Kontseiluak 2008ko apirilaren 10ean onartua, 13, 14 eta 18. artikuluak.

V.– Erreklamazioak (eskubideen babesa):

• Eskatzaileak uste badu oztopoak jarri zaizkiola bere datuak atzitzeko eskubidea baliatu ahal izateko, erreklamazioa egin dezake Datuak Babesteko Euskal Bulegoan, bertan bere eskubideak babesteko prozedura abiaraz dezaten.

• Hori egin aurretik, bere datuak atzitzeko eskubidea baliatu ahal izateko eskaera egiten duen egunetik hilabete bat igaro beharko da, bitarte horretan erantzun garbirik jaso gabe.

• Erreklamazioa Datuak Babesteko Euskal Bulegoari zuzenduko zaio (Tomas Zumarraga Dohatsuaren kalea 71, 3a - 01008 Vitoria-Gasteiz - Tel. 945 01 62 30 - Faxa: 945 01 62 31, avpd@avpd.es), eta agiri hauek aurkeztuko dira:

– Eskatutako informazioa emateari DBLO segurtasun-arduradunak egindako ukoa.

– Atzipen-eskaera egiteko ereduaren kopia, UPV/EHUren erregistroko sarrera-zigiluarekin.

– Posta-bulegoko zigiluaren kopia, eskaera ohiko postaz egin bada.

• La información deberá contener de modo legible e inteligible los datos incluidos en el fichero y los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los datos, los cesionarios (instituciones y organizaciones públicas o privadas a los que se ha comunicado o se prevé comunicar tales datos) y la especificación de los usos concretos y finalidades para los que se almacenaron.

• La entrega de datos es gratuita.

IV.– Normativa de aplicación:

• Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, artículo 15.

• Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, artículos 23, 24, 25, 26, 27, 28, 29 y 30.

• Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal y de creación de la Agencia Vasca de Protección de Datos, artículo 8 y 9.

• Decreto 308/2005, de 18 de octubre, por el que se desarrolla la Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos, artículos 6, 7 y 8.

• Reglamento de la UPV/EHU para la protección de datos de carácter personal, aprobado por el Consejo de Gobierno de la Universidad de 10 de abril de 2008, artículos 13, 14 y 18.

V.– Reclamaciones (Tutela de derechos):

• Si el o la solicitante entiende que no se le ha facilitado correctamente el derecho de acceso a sus propios datos, puede reclamar ante la Agencia Vasca de Protección de Datos para que inicie un procedimiento de tutela de sus derechos.

• Para ello, resulta necesario que haya transcurrido el plazo de un mes desde la solicitud del derecho de acceso, sin que de forma expresa se le haya contestado.

• La reclamación se dirigirá a la Agencia Vasca de Protección de Datos (c/ Beato Tomás de Zumárraga, 71, 3º - 01008 Vitoria-Gasteiz - Tel. 945 01 62 30 - Fax. 945 01 62 31 avpd@avpd.es - www.avpd.es), aportándose alguno de los siguientes documentos:

– La negativa de la persona Responsable de Seguridad LOPD a facilitar la información solicitada.

– Copia del modelo de petición de acceso, sellada por el registro de entrada de la UPV/EHU.

– Copia del sello de la oficina de correos si la solicitud se ha remitido por correo ordinario.

ERANSKINA

I.V.E. DATUAK ZUZENTZEKO ESKUBIDEA

UPV/EHUREN FITXATEGIETAKO NIRE DATU PERTSONALAK ZUZENTZEKO ESKAERA

Nire datu pertsonalak zuzentzeko eskaerak ukitzen d(it)uen fitxategi(ar)ei buruzko datuak:

Fitxategi(ar)en izena(k)						
Nori zuzendua	EUSKAL HERRIKO UNIBERTSITATEA Informazio eta Komunikazio Teknologietarako Gerenteordetza Nori zuzendua: DBLO segurtasun-arduraduna					
Auzoa	Sarriena			Zk.	-	Solairua -
Herria	Leioa	Lurralde historikoa	Bizkaia		Posta-kodea	48940

Eskatzaileari buruzko datuak:

Abizenak						
Izena		NAN				
Kalea				Zk.		Solairua
Herria		Lurralde historikoa			Posta-kodea	
Telefonoa		Posta elektronikoa				

Legezko ordezkariari buruzko datuak:

Abizenak			
Izena		NAN	

Datu pertsonalak babesteari buruzko arautegian ezarritakoarekin bat etorriz, datuak zuzentzeko eskubidea baliatu nahi dut; beraz, ESKATZEN DUT:

1.– Aipatutako fitxategi(et)an dauden niri buruzko datu oker hauek zuzentzea:

Datu okerra	Datu zuzena

Edo erantsitako orrian adierazten ditudan datuak

2.– Azaldutako zuzenketa niri jakinaraztea.

3.– Nire datuen jakinarazpena jaso duten fitxategi edo tratamenduen pertsona erantzuleei jakinaraztea datuak zuzendu direla.

Tokia eta eguna	
Eskatzailearen sinadura	

ANEXO

I.M.V DERECHO DE RECTIFICACIÓN

SOLICITUD DE EJERCICIO DEL DERECHO DE RECTIFICACIÓN EN MIS DATOS DE CARÁCTER PERSONAL INSCRITOS EN FICHERO DE LA UPV/EHU

Datos del fichero/s en el/los que solicito la rectificación de mis datos de carácter personal:

Nombre del Fichero/s						
Dirigido a	*UNIVERSIDAD DEL PAÍS VASCO / EUSKAL HERRIKO UNIBERTSITATEA* *Vicegerencia de las Tecnologías de la Información y las Comunicaciones* *A la atención de: Responsable de Seguridad LOPD*					
Barrio	*Sarriena*			*N.º*	*-*	*Piso*	*-*
Localidad	*Leioa*	*Terr. Histórico*	*Bizkaia*		*Cód. Postal*	*48940*

Datos del o de la solicitante:

Apellidos					
Nombre		*DNI*			
Calle			*N.º*	*Piso*	
Localidad		*Terr. Histórico*		*Cód. Postal*	
Telefono		*Correo electrónico*			

Datos del o de la representante legal:

Apellidos			
Nombre		*DNI*	

Deseo ejercer mi derecho de rectificación, de conformidad con lo establecido en la normativa sobre protección de datos de carácter personal, por lo que SOLICITO se proceda a:

1.– La rectificación de los siguientes datos erróneos relativos a mi persona que se encuentran en el/los fichero/s referidos:

Dato erróneo	*Dato correcto*

O los datos que señalo en la hoja anexa

2.– Notificarme la rectificación planteada.

3.– Notificar a las personas responsables de los ficheros o tratamientos a quiénes hubieran sido comunicados los datos la rectificación practicada.

Lugar y fecha	
Firma del o de la solicitante	

INFORMAZIO OSAGARRIA

I.– Formularioa betetzeko eta idazkiari dokumentazioa eransteko argibideak:

• Formularioaren atal guztiak bete behar dira, eta formulario hori interesdunak izenpetu beharko du.

• Eskaerarekin batera aurkeztu beharko dira, behar izanez gero, datu berriak egiazkoak direla frogatuko duten dokumentuak.

• Beti aurkeztu behar da NANaren fotokopia edo interesduna identifikatuko duen beste edozein dokumentu baliodunena.

• Interesduna adin txikikoa bada edo ezgaiturik badago, bere ordezkari legalaren NANaren fotokopia aurkeztu beharko da, edo ordezkari hori identifikatuko duen beste edozein dokumentu baliodun; baita ordezkaritza legezkoa dela egiaztatzen duen benetako agiriaren fotokopia ere.

II.– Eskubidea baliatzen duenak jarraitu beharreko prozedura:

• Datuak zuzentzeko eskubidea baliatzeko idazki bat aurkeztu beharko zaio DBLO segurtasun-arduradunari, unibertsitateko erregistro orokorrean edo UPV/EHUko 2007ko maiatzaren 28ko erabakian zerrendatutako bulegoetan (2007ko abuztuaren 3ko EHAA, 149. zk.); bestela, Herri Administrazioen Araubide Juridikoaren eta Administrazio Prozedura Erkidearen azaroaren 26ko 30/1992 Legeko 38.4. artikuluak ezarritako bideak erabiliz ere aurkez daiteke idazkia.

• Idazkia bidali dela frogatze aldera, komeni da UPV/EHUko erregistroko sarrera-zigilua egiaztagiritzat gordetzea.

III.– Fitxategi edo tratamenduaren pertsona erantzuleak jarraitu beharreko prozedura:

• Pertsona erantzuleak gehienez hamar egun balioduneko epea izango du eskatzaileari erantzuteko, bere eskaera jasotzen duen egunetik kontatzen hasita.

• Epe hori amaitu eta datuak zuzentzeko eskaerari buruzko erantzun garbirik egon ez bada, eskaerari uko egin zaiola ulertuko da.

• Datuak zuzentzeko eskaera baietsi bada, pertsona erantzuleak eskaera hori jasotzen duen egunetik kontatzen hasi eta hamar egun balioduneko epean egin beharko du zuzenketa.

• Datuak zuzentzea doakoa da.

INFORMACIÓN COMPLEMENTARIA

I.– Instrucciones para la cumplimentación del formulario y documentación a aportar junto al escrito:

• Se deberá rellenar la totalidad de los apartados solicitados en el formulario y éste debe ser firmado por la persona interesada.

• Se deberán entregar los documentos que se acompañen a la solicitud y que acrediten, en caso de ser necesario, la veracidad de los nuevos datos.

• En todo caso, será necesario la entrega de la fotocopia de DNI o cualquier otro medio de identificación personal válido en derecho de la persona interesada.

• En el supuesto de que la persona interesada sea menor o esté incapacitada, será necesario la entrega también de la fotocopia de DNI o cualquier otro medio de identificación personal válido en derecho del o de la representante legal, debiéndose además en este caso presentar una fotocopia del documento acreditativo auténtico de la representación legal.

II.– Requisitos del procedimiento para el que ejercita el derecho:

• El derecho de rectificación se ejercerá mediante escrito dirigido a la persona Responsable de Seguridad LOPD, a través del Registro General de la Universidad en cualquiera de las oficinas enumeradas en la Resolución de la UPV/EHU de 28 de mayo de 2007 (BOPV n.º 149, de 3 de agosto de 2007), o por cualesquiera de los medios previstos en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

• Es aconsejable, desde el punto de vista probatorio, acreditar la remisión del escrito, mediante sello de entrada en el registro de la UPV/EHU.

III.– Requisitos del procedimiento para la persona Responsable del fichero o tratamiento:

• La persona responsable deberá responder al o a la solicitante en el plazo máximo de diez días hábiles, a contar desde la fecha de recepción de la solicitud.

• Transcurrido este plazo sin que de forma expresa se conteste a la petición de rectificación, ésta se entenderá denegada.

• Si la solicitud del derecho de rectificación fuese estimada, la persona responsable deberá rectificar en el plazo de diez días hábiles a contar desde la fecha de recepción de la solicitud.

• La rectificación de datos es gratuita.

IV.– Araudi aplikagarria:

• Datu Pertsonalak Babesteari buruzko 15/1999 Lege Organikoa, abenduaren 13koa, 16 artikulua.

• Abenduaren 21eko 1720/2007 Errege Dekretua, Datu Pertsonalak Babesteari buruzko abenduaren 13ko 15/1999 Lege Organikoa garatuko duen erregelamendua onartzen duena, 23, 24, 25, 26, 31, 32 eta 33. artikuluak.

• 2/2004 Legea, otsailaren 25ekoa, datu pertsonaletarako jabetza publikoko fitxategiei eta Datuak Babesteko Euskal Bulegoa sortzeari buruzkoa, 8. eta 9. artikuluak.

• 308/2005 Dekretua, urriaren 18koa, datu pertsonaletarako jabetza publikoko fitxategiei eta Datuak Babesteko Euskal Bulegoa sortzeari buruzko otsailaren 25eko 2/2004 Legea garatzen duena, 9. artikulua.

• Datu Pertsonalak Babesteari buruzko UPV/EHUren Arautegia, unibertsitateko Gobernu Kontseiluak 2008ko apirilaren 10ean onartua, 13, 15 eta 18. artikuluak.

V.– Erreklamazioak (eskubideen babesa):

• Eskatzaileak uste badu oztopoak jarri zaizkiola bere datuak zuzentzeko eskubidea baliatu ahal izateko, erreklamazioa egin dezake Datuak Babesteko Euskal Bulegoan, bertan bere eskubideak babesteko prozedura abiaraz dezaten.

• Hori egin aurretik, bere datuak zuzentzeko eskubidea baliatu ahal izateko eskaera egiten duen egunetik hamar egun igaro beharko dira, bitarte horretan erantzun garbirik jaso gabe.

• Erreklamazioa Datuak Babesteko Euskal Bulegoari zuzenduko zaio (Tomas Zumarraga Dohatsuaren kalea 71, 3a - 01008 Vitoria-Gasteiz - Tel. 945 01 62 30 - Faxa: 945 01 62 31, avpd@avpd.es), eta agiri hauek aurkeztuko dira:

– Fitxategi edo tratamenduaren pertsona erantzuleak eskatutako zuzenketari egindako ukoa.

– Zuzenketa-eskaera egiteko ereduaren kopia, UPV/EHUren erregistroko sarrera-zigiluarekin.

– Posta-bulegoko zigiluaren kopia, eskaera ohiko postaz egin bada.

IV.– Normativa de aplicación:

• Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, artículo 16.

• Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, artículos 23, 24, 25, 26, 31, 32 y 33.

• Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal y de creación de la Agencia Vasca de Protección de Datos, artículo 8 y 9.

• Decreto 308/2005, de 18 de octubre, por el que se desarrolla la Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos, artículo 9.

• Reglamento de la UPV/EHU para la protección de datos de carácter personal, aprobado por el Consejo de Gobierno de la Universidad de 10 de abril de 2008, artículos 13, 15 y 18.

V.– Reclamaciones (Tutela de derechos):

• Si el o la solicitante entiende que no se le ha facilitado correctamente el derecho de rectificación de sus propios datos, puede reclamar ante la Agencia Vasca de Protección de Datos para que inicie un procedimiento de tutela de sus derechos.

• Para ello, resulta necesario que haya transcurrido el plazo de diez días desde la solicitud del derecho de rectificación, sin que de forma expresa se le haya contestado.

• La reclamación se dirigirá a la Agencia Vasca de Protección de Datos (c/ Beato Tomás de Zumárraga, 71, 3.º - 01008 Vitoria-Gasteiz - Tel. 945 01 62 30 - Fax. 945 01 62 31 avpd@avpd.es - www.avpd.es), aportándose alguno de los siguientes documentos:

– La negativa de la persona Responsable del fichero o tratamiento a la rectificación solicitada.

– Copia del modelo de petición de rectificación, sellada por el registro de entrada de la UPV/EHU.

– Copia del sello de la oficina de correos si la solicitud se ha remitido por correo ordinario.

ERANSKINA

I.VI.E. DATUAK EZEREZTEKO ESKUBIDEA

UPV/EHUREN FITXATEGIETAKO NIRE DATU PERTSONALAK EZEREZTEKO ESKAERA

Nire datu pertsonalak ezerezteko eskaerak ukitzen d(it)uen fitxategi(ar)ei buruzko datuak:

Fitxategi(ar)en izena(k)						
Nori zuzendua	EUSKAL HERRIKO UNIBERTSITATEA Informazio eta Komunikazio Teknologietarako Gerenteordetza Nori zuzendua: DBLO segurtasun-arduraduna					
Auzoa	Sarriena		Zk.	-	Solairua	-
Herria	Leioa	Lurralde historikoa	Bizkaia		Posta-kodea	48940

Eskatzaileari buruzko datuak:

Abizenak						
Izena		NAN				
Kalea			Zk.		Solairua	
Herria		Lurralde historikoa			Posta-kodea	
Telefonoa		Posta elektronikoa				

Legezko ordezkariari buruzko datuak:

Abizenak			
Izena		NAN	

Datu pertsonalak babesteari buruzko arautegian ezarritakoarekin bat etorriz, datuak ezerezteko eskubidea baliatu nahi dut. Horretarako:

☐ Ezereztea justifikatzen duen dokumentazioa eransten dut.
☐ Lehenago agertutako adostasuna ezeztatzen dut, eta ez dut inolako dokumentaziorik eransten.

Beraz, ESKATZEN DUT:

1.– Aipatutako fitxategi(et)an dauden niri buruzko datuak ezereztea, ez baitago horiek gordetzea justifikatzen duen lotura juridiko edo lege-xedapenik.
2.– Eskatutako ezereztea burutu dela niri jakinaraztea.
3.– Nire datuen jakinarazpena jaso duten fitxategi edo tratamenduen pertsona erantzuleei jakinaraztea datuak ezereztu direla, haiek ere dagozkien aldaketak egin ditzaten.

Tokia eta eguna	
Eskatzailearen sinadura	

ANEXO

I.M.VI DERECHO DE CANCELACIÓN

SOLICITUD DE EJERCICIO DEL DERECHO DE CANCELACIÓN DE MIS DATOS DE CARÁCTER PERSONAL INSCRITOS EN FICHERO DE LA UPV/EHU

Datos del fichero/s en el/los que solicito la cancelación de mis datos de carácter personal:

Nombre del Fichero/s						
Dirigido a	*UNIVERSIDAD DEL PAÍS VASCO / EUSKAL HERRIKO UNIBERTSITATEA* *Vicegerencia de las Tecnologías de la Información y las Comunicaciones* *A la atención de: Responsable de Seguridad LOPD*					
Barrio	*Sarriena*		*N.º*	-	*Piso*	-
Localidad	*Leioa*	*Terr. Histórico*	*Bizkaia*		*Cód. Postal*	*48940*

Datos del o de la solicitante:

Apellidos					
Nombre		*DNI*			
Calle			*N.º*	*Piso*	
Localidad		*Terr. Histórico*		*Cód. Postal*	
Telefono		*Correo electrónico*			

Datos del o de la representante legal:

Apellidos			
Nombre		*DNI*	

Deseo ejercer mi derecho de cancelación, de conformidad con lo establecido en la normativa sobre protección de datos de carácter personal. Para ello:

☐ *Adjunto documentación justificativa de la cancelación.*
☐ *Revoco el consentimiento otorgado anteriormente, y no adjunto ninguna documentación adicional.*

Por lo que SOLICITO se proceda a:

1.– la cancelación de cualquier dato relativo a mi persona que se encuentre en el/los fichero/s referidos, al no existir vinculación jurídica o disposición legal que justifique su mantenimiento.
2.– notificarme la cancelación solicitada.
3.– notificar a los responsables de ficheros o tratamientos a quiénes hubieran sido comunicados los datos la cancelación para que ellos también procedan a realizar las modificaciones oportunas.

Lugar y fecha	
Firma del o de la solicitante	

INFORMAZIO OSAGARRIA

I.– Formularioa betetzeko eta idazkiari dokumentazioa eransteko argibideak:

• Formularioaren atal guztiak bete behar dira, eta formulario hori interesdunak izenpetu beharko du.

• Beharrezkoa da ezereztea justifikatzen duen dokumentazioa eranstea, edo, bestela, lehenago agertutako adostasuna ezeztatzea.

• Beti aurkeztu behar da NANaren fotokopia edo interesduna identifikatuko duen beste edozein dokumentu baliodunena.

• Interesduna adin txikikoa bada edo ezgaiturik badago, bere ordezkari legalaren NANaren fotokopia aurkeztu beharko da, edo ordezkari hori identifikatuko duen beste edozein dokumentu baliodun; baita ordezkaritza legezkoa dela egiaztatzen duen benetako agiriaren fotokopia ere.

II.– Eskubidea baliatzen duenak jarraitu beharreko prozedura:

• Datuak ezerezteko eskubidea baliatzeko idazki bat aurkeztu beharko zaio DBLO segurtasun-arduradunari, unibertsitateko erregistro orokorrean edo UPV/EHUko 2007ko maiatzaren 28ko erabakian zerrendatutako bulegoetan (2007ko abuztuaren 3ko EHAA, 149. zk.); bestela, Herri Administrazioen Araubide Juridikoaren eta Administrazio Prozedura Erkidearen azaroaren 26ko 30/1992 Legeko 38.4. artikuluak ezarritako bideak erabiliz ere aurkez daiteke idazkia.

• Idazkia bidali dela frogatze aldera, komeni da UPV/EHUko erregistroko sarrera-zigilua egiaztagiritzat gordetzea.

III.– Fitxategi edo tratamenduaren pertsona erantzuleak jarraitu beharreko prozedura:

• Pertsona erantzuleak gehienez hamar egun baliodunako epea izango du eskatzaileari erantzuteko, bere eskaera jasotzen duen egunetik kontatzen hasita.

• Epe hori amaitu eta datuak ezerezteko eskaerari buruzko erantzun garbirik egon ez bada, eskaerari uko egin zaiola ulertuko da.

• Datuak ezerezteko eskaera baietsi bada, pertsona erantzuleak eskaera hori jasotzen duen egunetik kontatzen hasi eta hamar egun balioduneko epean ezereztu beharko ditu.

• Ezerezteak datuak blokeatzea ekarriko du; alabaina, datu horiek administrazio publikoen, epaileen eta auzitegien esku egoten jarraituko dute, datuen tratamenduaren ondorioz sor daitezkeen erantzukizunak aintzat hartzeko, erantzukizun horien preskripzio-epeak iraun bitartean. Epe hori amaitu ondoren, datuak behin be-

INFORMACIÓN COMPLEMENTARIA

I.– Instrucciones para la cumplimentación del formulario y documentación a aportar junto al escrito:

• Se deberá rellenar la totalidad de los apartados solicitados en el formulario y éste debe ser firmado por la persona interesada.

• En necesario adjuntar documentación justificativa de la cancelación o, en su caso, revocar el consentimiento otorgado anteriormente.

• En todo caso, será necesario la entrega de la fotocopia de DNI o cualquier otro medio de identificación personal válido en derecho de la persona interesada.

• En el supuesto de que la persona interesada sea menor o esté incapacitada, será necesario la entrega también de la fotocopia de DNI o cualquier otro medio de identificación personal válido en derecho del o de la representante legal, debiéndose además en este caso presentar una fotocopia del documento acreditativo auténtico de la representación legal.

II.– Requisitos del procedimiento para el que ejercita el derecho:

• El derecho de cancelación se ejercerá mediante escrito dirigido a la persona Responsable de Seguridad LOPD, a través del Registro General de la Universidad en cualquiera de las oficinas enumeradas en la Resolución de la UPV/EHU de 28 de mayo de 2007 (BOPV n.º 149, de 3 de agosto de 2007), o por cualesquiera de los medios previstos en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

• Es aconsejable, desde el punto de vista probatorio, acreditar la remisión del escrito, mediante sello de entrada en el registro de la UPV/EHU.

III.– Requisitos del procedimiento para la persona Responsable del fichero o tratamiento:

• La persona responsable deberá responder al o a la solicitante en el plazo máximo de diez días hábiles, a contar desde la fecha de recepción de la solicitud.

• Transcurrido este plazo sin que de forma expresa se conteste a la petición de cancelación, ésta se entenderá denegada.

• Si la solicitud del derecho de cancelación fuese estimada, la persona responsable deberá cancelar los datos en el plazo de diez días hábiles a contar desde la fecha de recepción de la solicitud.

• La cancelación dará lugar al bloqueo de los datos conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse al borrado

tikoz ezabatzeari ekingo zaio, eta horren berri emango zaio interesdunari.

• Argi dagoenean ez dagoela datuen tratamendutik erator daitekeen erantzukizunik, datuak fisikoki ezabatuko dira. Hori egiterik ez badago, erantzuleak datuak blokeatu egingo ditu, inork erabili edo tratatu ez ditzan.

• Datuak ezereztea doakoa da.

IV.– Araudi aplikagarria:

• Datu Pertsonalak Babesteari buruzko 15/1999 Lege Organikoa, abenduaren 13koa, 16 artikulua.

• Abenduaren 21eko 1720/2007 Errege Dekretua, Datu Pertsonalak Babesteari buruzko abenduaren 13ko 15/1999 Lege Organikoa garatuko duen erregelamendua onartzen duena, 23, 24, 25, 26, 31, 32 eta 33. artikuluak.

• 2/2004 Legea, otsailaren 25ekoa, datu pertsonaletarako jabetza publikoko fitxategiei eta Datuak Babesteko Euskal Bulegoa sortzeari buruzkoa, 8. eta 9. artikuluak.

• 308/2005 Dekretua, urriaren 18koa, datu pertsonaletarako jabetza publikoko fitxategiei eta Datuak Babesteko Euskal Bulegoa sortzeari buruzko otsailaren 25eko 2/2004 Legea garatzen duena, 9. artikulua.

• Datu Pertsonalak Babesteari buruzko UPV/EHUren Arautegia, unibertsitateko Gobernu Kontseiluak 2008ko apirilaren 10ean onartua, 13, 16 eta 18. artikuluak.

V.– Erreklamazioak (eskubideen babesa):

• Eskatzaileak uste badu oztopoak jarri zaizkiola bere datuak ezerezteko eskubidea baliatu ahal izateko, erreklamazioa egin dezake Datuak Babesteko Euskal Bulegoan, bertan bere eskubideak babesteko prozedura abiaraz dezaten.

• Hori egin aurretik, bere datuak ezerezteko eskubidea baliatu ahal izateko eskaera egiten duen egunetik hamar egun igaro beharko dira, bitarte horretan erantzun garbirik jaso gabe.

• Erreklamazioa Datuak Babesteko Euskal Bulegoari zuzenduko zaio (Tomas Zumarraga Dohatsuaren kalea 71, 3a - 01008 Vitoria-Gasteiz - Tel. 945 01 62 30 - Faxa: 945 01 62 31, avpd@avpd.es), eta agiri hauek aurkeztuko dira:

– Fitxategi edo tratamenduaren pertsona erantzuleak eskatutako ezerezteari egindako ukoa.

– Datuak ezerezteko eskaera egiteko ereduaren kopia, UPV/EHUren erregistroko sarrera-zigiluarekin.

– Posta-bulegoko zigiluaren kopia, eskaera ohiko postaz egin bada.

definitivo y se volverá a informar a la persona interesada de ello.

• En los casos en los que claramente no existan potenciales responsabilidades nacidas del tratamiento, se procederá al borrado físico de los datos, excepto cuando la misma no sea materialmente posible, en cuyo caso la persona responsable procederá al bloqueo de los datos con el fin de impedir su utilización y tratamiento.

• La cancelación de datos es gratuita.

IV.– Normativa de aplicación:

• Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, artículo 16.

• Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, artículos 23, 24, 25, 26, 31, 32 y 33.

• Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal y de creación de la Agencia Vasca de Protección de Datos, artículo 8 y 9.

• Decreto 308/2005, de 18 de octubre, por el que se desarrolla la Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos, artículo 9.

• Reglamento de la UPV/EHU para la protección de datos de carácter personal, aprobado por el Consejo de Gobierno de la Universidad de 10 de abril de 2008, artículos 13, 16 y 18.

V.– Reclamaciones (Tutela de derechos):

• Si el o la solicitante entiende que no se le ha facilitado correctamente el derecho de cancelación de sus propios datos, puede reclamar ante la Agencia Vasca de Protección de Datos para que inicie un procedimiento de tutela de sus derechos.

• Para ello, resulta necesario que haya transcurrido el plazo de diez días desde la solicitud del derecho de cancelación, sin que de forma expresa se le haya contestado.

• La reclamación se dirigirá a la Agencia Vasca de Protección de Datos (c/ Beato Tomás de Zumárraga, 71, 3.º - 01008 Vitoria-Gasteiz - Tel. 945 01 62 30 - Fax. 945 01 62 31 avpd@avpd.es - www.avpd.es), aportándose alguno de los siguientes documentos:

– La negativa de persona Responsable del fichero o tratamiento a la cancelación solicitada.

– Copia del modelo de petición de cancelación, sellada por el registro de entrada de la UPV/EHU.

– Copia del sello de la oficina de correos si la solicitud se ha remitido por correo ordinario.

ERANSKINA

I.VII.E. DATUEN AURKA EGITEKO ESKUBIDEA

UPV/EHUREN FITXATEGIETAKO NIRE DATU PERTSONALAK TRATATZEAREN AURKA EGITEKO ESKAERA

Nire datu pertsonalak tratatzearen aurka egiteak ukitzen d(it)uen fitxategi(ar)ei buruzko datuak:

Fitxategi(ar)en izena(k)						
Nori zuzendua	EUSKAL HERRIKO UNIBERTSITATEA Informazio eta Komunikazio Teknologietarako Gerenteordetza Nori zuzendua: DBLO segurtasun-arduraduna					
Auzoa	Sarriena			Zk.	-	Solairua -
Herria	Leioa	Lurralde historikoa	Bizkaia		Posta-kodea	48940

Eskatzaileari buruzko datuak:

Abizenak					
Izena		NAN			
Kalea			Zk.		Solairua
Herria		Lurralde historikoa		Posta-kodea	
Telefonoa		Posta elektronikoa			

Legezko ordezkariari buruzko datuak:

Abizenak			
Izena		NAN	

Datu pertsonalak babesteari buruzko arautegian ezarritakoarekin bat etorriz, aipatutako fitxategi(et)an dauden nire datu pertsonalak tratatzearen aurka egiteko eskubidea baliatu nahi dut; izan ere, nire egoera pertsonal zehatz bati dagozkion bidezko zio arrazoituak dauzkat horretarako, jarraian ematen ditudan arrazoiek erakusten duten moduan.

Nire arrazoibidea

Modu desegokian tratatzen ari diren datu pertsonalen deskribapena

Zergatik da desegokia tratamendua

Nire arrazoibidea egiaztatzeko eransten dudan dokumentazioa

Beraz, lehen adierazitako moduan aurka egiteko eskubidea onartzea ESKATZEN DUT.

Tokia eta eguna	
Eskatzailearen sinadura	

ANEXO

I.M.VII DERECHO DE OPOSICIÓN

SOLICITUD DE EJERCICIO DEL DERECHO DE OPOSICIÓN A QUE SE TRATEN MIS DATOS DE CARÁCTER PERSONAL INSCRITOS EN FICHERO DE LA UPV/EHU

Datos del fichero/s en el/los que me opongo al tratamiento de mis datos de carácter personal:

Nombre del Fichero/s	

Dirigido a	*UNIVERSIDAD DEL PAÍS VASCO / EUSKAL HERRIKO UNIBERTSITATEA* *Vicegerencia de las Tecnologías de la Información y las Comunicaciones* *A la atención de: Responsable de Seguridad LOPD*						
Barrio	*Sarriena*			*N.º*	-	*Piso*	-
Localidad	*Leioa*	*Terr. Histórico*	*Bizkaia*		*Cód. Postal*	*48940*	

Datos del o de la solicitante:

Apellidos					
Nombre		*DNI*			
Calle			*N.º*		*Piso*
Localidad		*Terr. Histórico*		*Cód. Postal*	
Telefono		*Correo electrónico*			

Datos del o de la representante legal:

Apellidos			
Nombre		*DNI*	

Deseo ejercer mi derecho de oposición al tratamiento de mis datos en los referidos ficheros, por existir motivos fundados y legítimos relativos a una concreta situación personal, de conformidad con lo establecido en la normativa sobre protección de datos de carácter personal y lo argumentado a continuación.

Mi argumentación

Descripción de los datos de carácter personal que se están tratando de manera inadecuada

Porqué es inadecuado el tratamiento

Documentación que acompaño para acreditar mi argumentación

Por lo que SOLICITO que se acceda a mi derecho de oposición en los términos anteriormente expuestos.

Lugar y fecha	
Firma del o de la solicitante	

INFORMAZIO OSAGARRIA

I.– Formularioa betetzeko eta idazkiari dokumentazioa eransteko argibideak:

• Formularioaren atal guztiak bete behar dira, eta formulario hori interesdunak izenpetu beharko du.

• Egoera pertsonal zehatz bati dagozkion bidezko zio arrazoituak baliatzen badira, horiek egiaztatzen dituzten dokumentuen kopiak eman beharko zaizkio fitxategi edo tratamenduaren pertsona erantzuleari.

• Beti aurkeztu behar da NANaren fotokopia edo interesduna identifikatuko duen beste edozein dokumentu baliodunena.

• Interesduna adin txikikoa bada edo ezgaiturik badago, bere ordezkari legalaren NANaren fotokopia aurkeztu beharko da, edo ordezkari hori identifikatuko duen beste edozein dokumentu baliodun; baita ordezkaritza legezkoa dela egiaztatzen duen benetako agiriaren fotokopia ere.

II.– Eskubidea baliatzen duenak jarraitu beharreko prozedura:

• Aurka egiteko eskubidea baliatzeko idazki bat aurkeztu beharko zaio DBLO segurtasun-arduradunari, unibertsitateko erregistro orokorrean edo UPV/EHUko 2007ko maiatzaren 28ko erabakian zerrendatutako bulegoetan (2007ko abuztuaren 3ko EHAA, 149. zk.); bestela, Herri Administrazioen Araubide Juridikoaren eta Administrazio Prozedura Erkidearen azaroaren 26ko 30/1992 Legeko 38.4. artikuluak ezarritako bideak erabiliz ere aurkez daiteke idazkia.

• Idazkia bidali dela frogatze aldera, komeni da UPV/EHUko erregistroko sarrera-zigilua egiaztagiritzat gordetzea.

III.– Fitxategi edo tratamenduaren pertsona erantzuleak jarraitu beharreko prozedura:

• Pertsona erantzuleak gehienez hamar egun balioduneko epea izango du eskatzaileari erantzuteko, bere eskaera jasotzen duen egunetik kontatzen hasita.

• Epe hori amaitu eta aurka egiteko eskaerari buruzko erantzun garbirik egon ez bada, eskaerari uko egin zaiola ulertuko da.

• Aurka egiteko eskaera baietsi bada, pertsona erantzuleak eskaera hori jasotzen duen egunetik kontatzen hasi eta hamar egun balioduneko epean baztertu beharko d(it)u eskatzaileak adierazitako tratamendua(k).

• Datuen tratamendua baztertzea doakoa da.

INFORMACIÓN COMPLEMENTARIA

I.– Instrucciones para la cumplimentación del formulario y documentación a aportar junto al escrito:

• Se deberá rellenar la totalidad de los apartados solicitados en el formulario y éste debe ser firmado por la persona interesada.

• En el caso de que se trate motivos fundados y legítimos relativos a una concreta situación personal es necesaria la aportación de copias de documentos que lo acrediten a la persona Responsable del fichero o tratamiento.

• En todo caso, será necesario la entrega de la fotocopia de DNI o cualquier otro medio de identificación personal válido en derecho de la persona interesada.

• En el supuesto de que la persona interesada sea menor o esté incapacitada, será necesario la entrega también de la fotocopia de DNI o cualquier otro medio de identificación personal válido en derecho del o de la representante legal, debiéndose además en este caso presentar una fotocopia del documento acreditativo auténtico de la representación legal.

II.– Requisitos del procedimiento para el que ejercita el derecho:

• El derecho de oposición se ejercerá mediante escrito dirigido a la persona Responsable de Seguridad LOPD, a través del Registro General de la Universidad en cualquiera de las oficinas enumeradas en la Resolución de la UPV/EHU de 28 de mayo de 2007 (BOPV n.º 149, de 3 de agosto de 2007), o por cualesquiera de los medios previstos en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

• Es aconsejable, desde el punto de vista probatorio, acreditar la remisión del escrito, mediante sello de entrada en el registro de la UPV/EHU.

III.– Requisitos del procedimiento para la persona Responsable del fichero o tratamiento:

• La persona responsable deberá responder al o a la solicitante en el plazo máximo de diez días hábiles, a contar desde la fecha de recepción de la solicitud.

• Transcurrido este plazo sin que de forma expresa se conteste a la petición de oposición, ésta se entenderá denegada.

• Si la solicitud del derecho de oposición fuese estimada, la persona responsable deberá excluir el tratamiento o tratamientos a que se refiera en el plazo de diez días hábiles a contar desde la fecha de recepción de la solicitud.

• La exclusión del tratamiento de datos es gratuita.

IV.– Araudi aplikagarria:

• Datu Pertsonalak Babesteari buruzko 15/1999 Lege Organikoa, abenduaren 13koa, 6.4 eta 17. artikuluak.

• Abenduaren 21eko 1720/2007 Errege Dekretua, Datu Pertsonalak Babesteari buruzko abenduaren 13ko 15/1999 Lege Organikoa garatuko duen erregelamendua onartzen duena, 23, 24, 25, 26, 34, 35 eta 36. artikuluak.

• 2/2004 Legea, otsailaren 25ekoa, datu pertsonaletarako jabetza publikoko fitxategiei eta Datuak Babesteko Euskal Bulegoa sortzeari buruzkoa, 8. eta 9. artikuluak.

• 308/2005 Dekretua, urriaren 18koa, datu pertsonaletarako jabetza publikoko fitxategiei eta Datuak Babesteko Euskal Bulegoa sortzeari buruzko otsailaren 25eko 2/2004 Legea garatzen duena, 5. artikulua.

• Datu Pertsonalak Babesteari buruzko UPV/EHUren Arautegia, unibertsitateko Gobernu Kontseiluak 2008ko apirilaren 10ean onartua, 13, 17 eta 18. artikuluak.

V.– Erreklamazioak (eskubideen babesa):

• Eskatzaileak uste badu oztopoak jarri zaizkiola datuen aurka egiteko duen eskubidea baliatu ahal izateko, erreklamazioa egin dezake Datuak Babesteko Euskal Bulegoan, bertan bere eskubideak babesteko prozedura abiaraz dezaten.

• Hori egin aurretik, aurka egiteko eskubidea baliatu ahal izateko eskaera egiten duen egunetik hamar egun igaro beharko dira, bitarte horretan erantzun garbirik jaso gabe.

• Erreklamazioa Datuak Babesteko Euskal Bulegoari zuzenduko zaio (Tomas Zumarraga Dohatsuaren kalea 71, 3ª - 01008 Vitoria-Gasteiz - Tel. 945 01 62 30 - Faxa: 945 01 62 31, avpd@avpd.es), eta agiri hauek aurkeztuko dira:

– Fitxategi edo tratamenduaren pertsona erantzuleak tratamendua baztertzeko jaso duen eskaerari egindako ukoa.

– Aurka egiteko eskaera-ereduaren kopia, UPV/EHUren erregistroko sarrera-zigiluarekin.

– Posta-bulegoko zigiluaren kopia, eskaera ohiko postaz egin bada.

IV.– Normativa de aplicación:

• Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, artículos 6.4, y 17.

• Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, artículos 23, 24, 25, 26, 34, 35 y 36.

• Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal y de creación de la Agencia Vasca de Protección de Datos, artículo 8 y 9.

• Decreto 308/2005, de 18 de octubre, por el que se desarrolla la Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos, artículo 5.

• Reglamento de la UPV/EHU para la protección de datos de carácter personal, aprobado por el Consejo de Gobierno de la Universidad de 10 de abril de 2008, artículos 13, 17 y 18.

V.– Reclamaciones (Tutela de derechos):

• Si el o la solicitante entiende que no se le ha facilitado correctamente el derecho de oposición de sus propios datos, puede reclamar ante la Agencia Vasca de Protección de Datos para que inicie un procedimiento de tutela de sus derechos.

• Para ello, resulta necesario que haya transcurrido el plazo de diez días desde la solicitud del derecho de oposición, sin que de forma expresa se le haya contestado.

• La reclamación se dirigirá a la Agencia Vasca de Protección de Datos (c/ Beato Tomás de Zumárraga, 71, 3.º - 01008 Vitoria-Gasteiz - Tel. 945 01 62 30 - Fax. 945 01 62 31 avpd@avpd.es - www.avpd.es), aportándose alguno de los siguientes documentos:

– La negativa de la persona Responsable del fichero o tratamiento a la exclusión del tratamiento solicitada.

– Copia del modelo de petición de oposición, sellada por el registro de entrada de la UPV/EHU.

– Copia del sello de la oficina de correos si la solicitud se ha remitido por correo ordinario.

ERANSKINA

I.VIII.E. UPV/EHUK AITORTU DITUEN DATU PERTSONALEN FITXATEGIAK

Jarraian Datuak Babesteko Euskal Bulegoan erregistraturik dauden UPV/EHUren datu pertsonalen fitxategiak aurkezten dira, unibertsitateko datu pertsonalen fitxategiak sortu, aldatu eta ezabatzeari buruz UPV/EHUren Gobernu Kontseiluak 2007ko otsailaren 8an hartutako erabakiari jarraiki [UPV/EHUko idazkari nagusiaren 2007ko otsailaren 28ko erabakiz argitaratua (2007ko apirilaren 11ko EHAA, 69. zk.)] aitortutakoak.

1.– Unibertsitaterako sarrera. Unibertsitatean sartzeko prozesuen kudeaketa.

2.– Lehen eta bigarren zikloko matrikulazioa. Unibertsitateko lehen eta bigarren zikloetan matrikula egiteko prozesuak kudeatzea.

3.– Hirugarren zikloko matrikulazioa. Unibertsitateko master eta graduondoko ikastaroetako matrikulazioa.

4.– Bekak eta laguntzak. Unibertsitateko bekak eta laguntzak eskatzen dituen jendearen datuak.

5.– Unibertsitate-tituluen bidalketa. Unibertsitate-tituluen kudeaketa.

6.– Ikasketa propioak. Ikasketa propioak egiten dituzten ikasleen matrikula eta espedienteak kudeatzea.

7.– Hirugarren ziklorako sarrera. Unibertsitateko graduondoko ikastaroetan sartzeko prozesuen kudeaketa.

8.– Doktoregoen kudeaketa. Unibertsitatean doktorego-tesia defendatzen duten ikasleen datu akademikoak eta kalifikazioak.

9.– Espediente akademikoak. Espediente akademikoak kudeatzea.

10.– Nominak. Nominak eta Gizarte Segurantzako kotizazioak kudeatzea.

11.– Gizarte-funtsa. Osasun-gastuak finantzatzeko laguntzak emateko erabiltzen den gizarte-funtsa kudeatzea.

12.– Langileen espedienteak. Giza baliabideak kudeatzea. Unibertsitateko giza baliabideak kudeatzea, unibertsitateko langileak aukeratzea eta administratzea.

13.– Kontsumo-kredituak. Unibertsitateko langileei kredituak emateko funtsa.

14.– Lanpostuak aukeratzea eta hornitzea. Lan-poltsak eta lanpostuak eskuratzeko eta hornitzeko deialdiak.

ANEXO

I.M.VIII. FICHEROS DE CARÁCTER PERSONAL DECLARADOS POR LA UPV/EHU

A continuación, se presentan los ficheros de carácter personal de la UPV/EHU inscritos en la Agencia Vasca de Protección de Datos en virtud del Acuerdo adoptado por el Consejo de Gobierno de la UPV/EHU de 8 de febrero de 2007 para la creación, modificación y supresión de ficheros de datos de carácter personal de la Universidad, publicado por Resolución de 28 de febrero de 2007 del Secretario General de la UPV/EHU (BOPV n.º 69, de 11 de abril de 2007).

1.– Acceso a la Universidad. Gestión de los procesos de acceso a la Universidad.

2.– Matriculación en primer y segundo ciclo. Gestión de los procesos de matriculación en primer y segundo ciclo de la Universidad.

3.– Matriculación en tercer ciclo. Matriculación en masters y cursos de postgrado de la Universidad.

4.– Becas y Ayudas. Datos de las personas que solicitan becas y ayudas de la Universidad.

5.– Expedición de títulos universitarios. Gestión de los títulos universitarios.

6.– Enseñanzas Propias. Gestión de la matrícula y de los expedientes del alumnado que cursa enseñanzas propias.

7.– Acceso a Tercer Ciclo. Gestión de los procesos de acceso a los cursos de postgrado de la Universidad.

8.– Gestión de Doctorado. Datos académicos y calificaciones del alumnado que lee su tesis doctoral en la Universidad.

9.– Expedientes Académicos. Gestión de expedientes académicos.

10.– Nóminas. Gestión de Nóminas y cotizaciones a la Seguridad Social.

11.– Fondo Social. Gestión del Fondo Social para la prestación de ayudas para financiar gastos de carácter sanitario.

12.– Expediente de personal. Gestión de recursos humanos. Gestión de los recursos humanos de la Universidad, Selección y administración de personal de la Universidad.

13.– Créditos de Consumo. Fondo para la prestación de créditos al personal de la Universidad.

14.– Selección y provisión de puestos. Bolsas de trabajo y convocatorias de acceso y provisión de puestos.

15.– Goi-mailako ikerkuntza. Ikerkuntza-xedeetarako fitxategia da; behar diren datu pertsonalak goi-mailari dagozkio.

16.– Ikerkuntza kudeatzea. Erakunde publiko eta pribatuek ikerkuntza-jarduerak egiteko ematen dituzten laguntzak eta diru-laguntzak kudeatzea eta bideratzea, Unibertsitateko sailek eta ikastegiek burututako ikerkuntza-jarduerari buruzko azterketak eta analisiak bilduz.

17.– Erdi-mailako ikerkuntza. Ikerkuntza-xedeetarako fitxategia da; behar diren datu pertsonalak maila ertainari dagozkio.

18.– Oinarrizko mailako ikerkuntza. Ikerkuntza-xedeetarako fitxategia da; behar diren datu pertsonalak oinarrizko mailari dagozkio.

19.– Enpresatako praktikak eta lan-poltsa. UPV/EHUko ikasleek enpresetan praktikak egin ditzaten eta UPV/EHUn ikasketak bukatu dituzten ikasleek enplegua topa dezaten erraztea.

20.– Erregistro orokorra. Dokumentuen sarrera- eta irteera-erregistroa.

21.– Idazkaritza Nagusia. Erabakiak, izendapenak, auzi judizialak eta beste administrazio batzuen eskakizunak kudeatzea.

22.– Hirugarrenen kudeaketa. Finantza-kudeaketa. Finantza-kudeaketaren, aurrekontu-kontabilitatearen eta finantza-kontabilitatearen gaineko datu-basea.

23.– Erosketak eta kontratazioa. Unibertsitateko hornitzaileak eta kontratistak.

24.– Hezkuntza-premia bereziak dituzten ikasleak. Hezkuntza-premia bereziak dituzten ikasleek unibertsitatean ikasketak egin ahal izan ditzaten behar diren egokitzapenak kudeatzea.

25.– Kirolak eta kultur jarduerak. Kultur jarduerak eta kirol ekitaldiak kudeatzea.

26.– Prebentzioa eta mediku-laguntza. Osasun-kontroletarako, mediku-azterketetarako, kontsulten segimendurako eta arriskuen prebentziorako behar diren datuak.

27.– Odontologiako klinikako bezeroak erregistratzea. UPV/EHUren odontologiako klinikaren administrazio- eta asistentzia-kudeaketa.

28.– Argitalpen-zerbitzua. Salmentak eta harpidetzak kudeatzea eta argitalpenak sustatzea.

29.– Fitxategi informatiko osagarria. Sistema eta domeinuetan erabiltzaileak baliozkotzea, hainbat aplikaziotan autentifikazioak erraztea eta, oro har, unibertsitateko baliabide informatikoen eta komunikazioen barne-kudeaketa burutzea.

30.– Liburutegia. Liburuen eta aldizkarien maileguak eta erreserbak kudeatzea.

15.– Investigación nivel alto. Fichero destinado a finalidades de investigación donde los datos de carácter personal necesarios se corresponden con el nivel alto.

16.– Gestión de la Investigación. Gestión y tramitación de todas las subvenciones y ayudas de entidades públicas y privadas destinadas a actividades de investigación, recopilando los estudios y análisis de la actividad investigadora desarrollada por los Departamentos y Centros de la Universidad.

17.– Investigación nivel medio. Fichero destinado a finalidades de investigación donde los datos de carácter personal necesarios se corresponden con el nivel medio.

18.– Investigación nivel básico. Fichero destinado a finalidades de investigación donde los datos de carácter personal necesarios se corresponden con el nivel básico.

19.– Prácticas en empresas y Bolsa de Empleo. Fichero destinado a facilitar la realización de prácticas en empresas de alumnado de la UPV/EHU y búsqueda de empleo de alumnado egresado de la misma.

20.– Registro General. Registro de entrada y salida de documentos.

21.– Secretaria General. Registro de resoluciones, nombramientos, designaciones, pleitos judiciales y requerimientos de otras administraciones.

22.– Gestión de terceros. Gestión financiera. Base de datos de gestión financiera, contabilidad presupuestaria y contabilidad financiera.

23.– Compras y contrataciones. Proveedores y contratistas de la Universidad.

24.– Alumnado con necesidades educativas especiales. Gestión de las adaptaciones necesarias para que el alumnado con necesidades educativas especiales pueda cursar sus estudios en la Universidad.

25.– Deportes y actividades culturales. Gestión de actividades deportivas y eventos culturales.

26.– Prevención y asistencia médica. Datos necesarios para el control sanitario, reconocimientos, seguimiento de consultas, prevención de riesgos.

27.– Registro de Pacientes de Clínica Odontológica. Gestión administrativa y asistencial de la Clínica Odontológica de la UPV/EHU.

28.– Servicio Editorial. Gestión de ventas, suscripciones y promoción editorial.

29.– Fichero auxiliar informático. Fichero destinado a validar usuarios en sistemas y dominios, facilitar autenticación en diversas aplicaciones, y en general a cualquier tipo de gestión interna de recursos informáticos y de comunicaciones de la universidad.

30.– Biblioteca. Gestión de préstamos y reservas de libros y revistas.

31.– Irakaskuntza-kalitateari buruzko galdeketak. Irakasleen gaineko iritzi- eta gogobetetze-galdeketak eta irakaskuntzarekin zerikusia duten galdeketa orokorrak kudeatzea.

32.– Protokoloa. UPV/EHUko protokolo-ekitaldien informazioa eta gonbidapenak bidaltzea.

33.– Mezenasgoa. Pertsona fisikoek unibertsitateari eginiko ekarpenen kudeaketa eta dagozkien ziurtagiriak ematea.

31.– Encuestas Calidad Docente. Gestión de las encuestas de opinión y satisfacción sobre el profesorado, así como encuestas sobre aspectos generales relacionados con la docencia.

32.– Protocolo. Envío de información, invitaciones a actos protocolarios de la UPV/EHU.

33.– Mecenazgo. Soporte en los procesos de que un particular realice aportaciones voluntarias a la Universidad y de las certificaciones necesarias.

ERANSKINA

I.IX.E. DBLOGEKO SEGURTASUN-NEURRIEN LABURPEN-KOADROA - FITXATEGI AUTOMATIZATUAK

<table>
<tr><td></td><td colspan="2">Oinarrizko maila: datu pertsonalen fitxategi edo tratamenduak</td></tr>
<tr><td></td><td colspan="2">Maila ertaina: administrazio-arloko edo zigor-arloko arau-hausteei buruzko datuen fitxategi edo tratamenduak; ondare-kaudimenaren eta kredituaren gaineko informazio-zerbitzua ematen dutenak; zerga-administrazioenak; finantza-erakundeenak; Gizarte Segurantzaren erakunde kudeatzaileen eta zerbitzu komunen ardurapean daudenak; lan-istripu eta gaixotasun profesionaletarako Gizarte Segurantzaren mutuetan daudenak eta, azkenik, izaeraren edo jokaeraren hainbat alderdi ebaluatzen dutenak.</td></tr>
<tr><td></td><td colspan="2">Goi-maila: ideologiari, erlijioari, sinesmenei, sindikatu-bazkidetzari, arrazari, osasunari, edo bizitza sexualari buruzko datuen fitxategi edo tratamenduak; interesdunaren adostasunik gabe, poliziaren xedeetarako bildutako datuak dituztenak eta, azkenik, genero-indarkeriaren ondoriozko datuak dituztenak.</td></tr>
<tr><td>Segurtasun-agiria</td><td>– Segurtasunari buruzko araudia ezartzen du eta honako hauek zehazten ditu: arau horien aplikazio-eremua; segurtasunari buruzko neurri, arau, prozedura eta estandarrak; langileen eginkizun eta betebeharrak; fitxategien eta informazio-sistemen deskribapena; segurtasun-gorabeherak kudeatzeko prozedurak; euskarriak, dokumentuak eta segurtasun-kopiak.
– Euskarri eta dokumentuak garraiatu, berrerabili edo baztertzerakoan hartu behar diren neurriak ezartzen ditu.
– Tratamenduaren eta fitxategien arduraduna identifikatzen du, eta hori guztia jasota geratzen da segurtasun-agirian eta kontratuan.
– Eguneraturik egon behar da, bai antolakuntzari bai indarreko legediari dagokionez.</td><td>– Segurtasun-arduradunak identifikatzen ditu
– Segurtasun-agirian ezarritakoa betetzen dela egiaztatzeko aldian behingo kontrolak ezartzen ditu.</td></tr>
<tr><td>Segurtasun-arduraduna</td><td></td><td>– Agirian jasotzen diren segurtasun-neurriak koordinatu eta kontrolatzeko ardura dauka.
– Horrek ez du esan nahi fitxategiaren erantzulea bere erantzukizunetik libratzen denik</td></tr>
<tr><td>Auditoretza</td><td></td><td>– Barne- edo kanpo-auditoretza egin beharko da gutxienez bi urtean behin,- eta sistema informatikoetan aldaketa garrantzitsuak gertatzen direnean.
– Auditoretzaren txostenak erabilitako neurriak egokiak diren erabakitzeko irizpidea ematen du, hutsuneak identifikatzen ditu, eta beharrezko neurri zuzentzaileak proposatzen ditu
– Auditoretzaren txostenak segurtasun-arduradunak aztertzen ditu
– Txosten horiek DBEBren esku uzten dira</td></tr>
<tr><td>Langileak</td><td colspan="2">– Segurtasun-agiriak langileen funtzio eta betebeharrei buruzko informazio argia eta zehatza biltzen du.
– Langileei beren eginkizunetan eragina duten segurtasun-neurriak eta horiek ez betetzeak dakartzan ondorioak jakinarazten zaizkie.</td></tr>
</table>

Identifikazioa eta autentifikazioa	– Erabiltzaileak identifikatu eta autentifikatzeko neurriak daude – Erabiltzaile bakoitzaren identifikazio uniboko eta pertsonala egiten da – Pasahitzak gorde eta banatzeko gestioak egiteko prozedura bat dago – Pasahitzen iraungipena kontrolatzeko eta pasahitzak modu ez-ulergarrian gordetzeko prozedura bat dago	– Baimendu gabeko atzipenak egiteko saiakeren kopurua murrizteko mekanismoa ezartzen da	
Atzipenen kontrola eta erregistroa	– Erabiltzaileek beren zereginak betetzeko behar dituzten datuak eta baliabideak baino ez dituzte atzitzen. – Erabiltzaileen, erabiltzaile-profilen eta baimendutako atzipenen zerrenda eguneratua dago – Baliabideak atzitzeko eskubideak kontrolatu ahal izateko mekanismo bat dago – Atzitzeko baimenak ematea gestionatzeko mekanismo bat dago, segurtasun-agiriaren arabera baimen horiek eman ahal dituzten langileek baizik eman ez ditzaten.	– Informazio-sistemak dauden lokaletan fisikoki sartzea kontrolatu egiten da.	– Atzipen-saiakera bakoitzari buruzko datuak erregistratzen dira. – Datuak bi urtez gordetzen dira. – Segurtasun-arduradunaren kontrolpean dago – Segurtasun-arduradunak hilero txostena egiten du – Salbuespena dago: pertsona fisikoa izatea eta berak baino ez atzitzea
Euskarri eta dokumentuen gestioa eta banaketa	– Daukaten informazio-mota identifikatzen da – nbentarioa gordetzen da – Atzipen murriztuarekin gordetzen dira – Fitxategiaren erantzuleak euskarrien irteera baimentzen du – Euskarriak baztertu behar direnean, neurriak hartzen dira	– Euskarrien sarrera eta irteeren erregistroa dago, argibide hauek ematen dituena: euskarri edo dokumentu mota, data eta ordua, igorlea edo hartzailea, informazio-mota, igorpen-mota eta pertsona erantzulea	– Erabiltzaile baimenduek baino ulertu ezin duten etiketatze-sistema bat dago – Datuak zifratu egiten dira, euskarriak banatzerakoan edo datuak gailu eramangarrietan lekualdatzerakoan
Segurtasun eta berreskurapen kopiak	– Datuen segurtasun-kopia egiteko eta datuak berreskuratzeko prozedura bat egon behar da – Datuak berreskuratzeko ezarritako prozedurak bermatu beharko du datuak galdu edo suntsitu zirenean zeuden bezala utziko dituela berriz ere – Segurtasun-kopia bat egiten da, gutxienez astean behin – Fitxategiaren erantzuleak sei hilean behin egiaztatuko ditu kopiak egiteko prozedurak – Datu errealak erabiliko dira, baldin eta tratatzen den fitxategiari dagokion segurtasun-maila ziurtatzen bada, eta kopia bat egin bada		– Segurtasun-kopia bat eta datuak berreskuratzeko prozeduren kopia bat gordeko da datuen tratamendurako tresna informatikorik ez dagoen lekuan
Gorabeheren erregistroa	– Honako hauek erregistratu beharko dira: nolako gorabehera izan den, noiz gertatu den, gorabeheraren jakinarazpena nork nori egin dion eta jakinarazpen horrek zer ondorio izan dituen	– Erregistroan datuak berreskuratzeko prozedurak ere jaso behar dira, honako hauek adieraziz: prozedura burutu duen pertsona, berreskuratutako datuak, eta berreskurapen-prozeduran eskuz grabatu behar izan diren datuak – Fitxategi edo tratamenduaren erantzuleak ematen du baimena datuak berreskuratzeko prozedurak burutzeko	
Telekomunikazioak	– Komunikazio-sareen bidezko datuen atzipenei eskatuko zaizkien segurtasun-neurriek bermatu beharreko segurtasun-maila atzipen lokalekoek bermatu beharrekoaren parekoa izango da		– Sare publikoen edo haririk gabeko sareen bidezko komunikazio elektronikoen bitartez transmititutako datuak zifratu egingo dira

ERANSKINA

I.X.E. DBLOGEKO SEGURTASUN-NEURRIEN LABURPEN-KOADROA - FITXATEGI EZ-AUTOMATIZATUAK

	Oinarrizko maila: datu pertsonalen fitxategi edo tratamenduak
	Maila ertaina: administrazio-arloko edo zigor-arloko arau-hausteei buruzko datuen fitxategi edo tratamenduak; ondarekaudimenaren eta kredituaren gaineko informazio-zerbitzua ematen dutenak; zerga-administrazioenak; finantza-erakundeenak; Gizarte Segurantzaren erakunde kudeatzaileen eta zerbitzu komunen ardurapean daudenak; lan-istripu eta gaixotasun profesionaletarako Gizarte Segurantzaren mutuetan daudenak eta, azkenik, izaeraren edo jokaeraren hainbat alderdi ebaluatzen dutenak.
	Goi-maila: ideologiari, erlijioari, sinesmenei, sindikatu-bazkidetzari, arrazari, osasunari, edo bizitza sexualari buruzko datuen fitxategi edo tratamenduak; interesdunaren adostasunik gabe, poliziaren xedeetarako bildutako datuak dituztenak eta, azkenik, genero-indarkeriaren ondoriozko datuak dituztenak.
Segurtasun-agiria	– Segurtasunari buruzko araudia ezartzen du eta honako hauek zehazten ditu: arau horien aplikazio-eremua; segurtasunari buruzko neurri, arau, prozedura eta estandarrak; langileen eginkizun eta betebeharrak; fitxategien eta informazio-sistemen deskribapena; segurtasun-gorabeherak kudeatzeko prozedurak; euskarriak, dokumentuak eta segurtasun-kopiak. – Euskarri eta dokumentuak garraiatu, berrerabili edo baztertzerakoan hartu behar diren neurriak ezartzen ditu. – Tratamenduaren eta fitxategien arduraduna identifikatzen du, eta hori guztia jasota geratzen da segurtasun-agirian eta kontratuan. – Eguneraturik egon behar da, bai antolakuntzari bai indarreko legediari dagokionez.
Langileak	– Segurtasun-agiriak langileen funtzio eta betebeharrei buruzko informazio argia eta zehatza biltzen du. – Langileei beren eginkizunetan eragina duten segurtasun-neurriak eta horiek ez betetzeak dakartzan ondorioak jakinarazten zaizkie.
Gorabeheren erregistroa	Honako hauek erregistratu beharko dira: nolako gorabehera izan den, noiz gertatu den, gorabeheraren jakinarazpena nork nori egin dion eta jakinarazpen horrek zer ondorio izan dituen
Atzipenen kontrola eta erregistroa	– Erabiltzaileek beren zereginak betetzeko behar dituzten datuak eta baliabideak baino ez dituzte atzitzen. – Erabiltzaileen, erabiltzaile-profilen eta baimendutako atzipenen zerrenda eguneratua dago – Baliabideak atzitzeko eskubideak kontrolatu ahal izateko mekanismo bat dago – Atzitzeko baimenak ematea gestionatzeko mekanismo bat dago, segurtasun-agiriaren arabera baimen horiek eman ahal dituzten langileek baizik eman ez ditzaten.
Euskarri eta dokumentuen gestioa	– Daukaten informazio-mota identifikatzen da – Inbentarioa gordetzen da – Atzipen murriztuarekin gordetzen dira – Fitxategiaren erantzuleak euskarrien irteera baimentzen du – Euskarriak baztertu behar direnean, neurriak hartzen dira
Artxiborako irizpideak	Irizpide horiek bermatu beharko dute dokumentuen kontserbazio egokia eta informazioaren lokalizazioa eta kontsulta, eta datuak atzitu, zuzendu, ezeztu edo datuen aurka egiteko eskubideak baliatzeko aukera eman beharko dute
Datuak gordetzeko gailuak	Gailuak irekitzea galaraziko duten mekanismoak izan beharko dituzte

Euskarrien zaintza	Datu pertsonalak dituen dokumentazioa dagokion gailuan artxibaturik ez dagoenean, zaindu egin beharko da		
Segurtasun arduraduna		– Agirian jasotzen diren segurtasun-neurriak koordinatu eta kontrolatzeko ardura dauka. – Horrek ez du esan nahi fitxategiaren erantzulea bere erantzukizunetik libratzen denik	
Auditoretza		– Barne- edo kanpo-auditoretza egin beharko da gutxienez bi urtean behin, eta sistema informatikoetan aldaketa garrantzitsuak gertatzen direnean. – Auditoretzaren txostenak erabilitako neurriak egokiak diren erabakitzeko irizpidea ematen du, hutsuneak identifikatzen ditu, eta beharrezko neurri zuzentzaileak proposatzen ditu – Auditoretzaren txostenak segurtasun-arduradunak aztertzen ditu – Txosten horiek DBEBren esku uzten dira	
Informazioa biltegiratzea			Sarrera giltzaz edo bestelako sistema batez babesturik duten agiritegiak
Kopia edo erreprodukzioa			– Segurtasun-agiriaren arabera bimena dutenek baino ez – Baztertutako kopiak suntsitu egin behar dira
Dokumentazioa atzitzea			– Baimendutako langileek baino ez – Atzipenak identifikatzeko mekanismoa dago – Baimendu gabeko atzipenen erregistroa dago
Dokumentazioa lekualdatzea			Atzipena edo manipulazioa galarazteko neurriak hartzen dira

ANEXO

I.M.IX. RESUMEN MEDIDAS DE SEGURIDAD RDLOPD - FICHEROS AUTOMATIZADOS

	Nivel básico: ficheros o tratamientos de datos de carácter personal	
	Nivel medio: ficheros o tratamientos de datos relativos a infracciones administrativas o penales, los que informen de servicios de solvencia patrimonial y crédito, los que sean de Administraciones tributarias, los de prestación de servicios financieros, los de las Entidades Gestoras y Servicios Comunes de la Seguridad Social, los de las mutuas de accidentes de trabajo y los que permitan evaluar la personalidad	
	Nivel alto: ficheros o tratamientos de datos relativos a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas y los que contengan datos derivados de actos de violencia de género	
Documento de seguridad	*– Implanta la normativa de seguridad concretando el ámbito de aplicación del mismo, las medidas, normas, procedimientos y estándares de seguridad, las funciones y obligaciones del personal, la descripción de los ficheros y de los SSII y los procedimientos de gestión de incidencias, soportes y documentos y copias de seguridad* *– Establece las medidas a adoptar en caso de transporte, reutilización o desecho de soportes y documentos* *– Identifica al encargado del tratamiento y los ficheros afectados y esto se expresa en el DS y en el contrato* *– Se debe mantener actualizado tanto en lo relativo a la organización como a la legislación vigente*	*– Identifica al o los responsables de seguridad* *– Establece los controles periódicos de cumplimiento del documento*
Responsable de seguridad		*– Es el encargado de coordinar y controlar las medidas de seguridad del documento* *– Esto no supone exoneración de la responsabilidad del responsable del fichero*
Auditoria		*– Una interna o externa al menos cada 2 años o cuando se realicen cambios sustanciales en los SSII* *– Da lugar a un informe de auditoría sobre la adecuación a las medidas, las deficiencias identificadas y propone medidas correctoras* *– Es analizado por el responsable de seguridad* *– Queda a disposición de la AVPD*
Personal	*– El Documento de Seguridad especifica las funciones y obligaciones de un modo claro y documentado* *– Se difunden entre el personal las normas que les afecten y las consecuencias por incumplimiento*	

Identificación y autenticación	*– Existen medidas para la identificación y autenticación de los usuarios* *– Se identifica unívoca y personalmente a cada usuario* *– Existe un procedimiento de gestión almacenamiento y distribución de contraseñas* *– Existe un procedimiento para controlar la caducidad de contraseñas y el almacenamiento ininteligible de las mismas*	*– Se establece un mecanismo que limite el número de intentos reiterados de acceso no autorizado*	
Control y registro de accesos	*– Cada usuario accede únicamente a los datos y recursos necesarios para el desarrollo de sus funciones* *– Existe una relación actualizada de usuarios, perfiles y accesos autorizados* *– Existen mecanismos para controlar los derechos con que se accede a los recursos* *– Existen mecanismos que gestionen la concesión de permisos de acceso sólo por personal autorizado en el Documento de Seguridad*	*– Se realiza un control de acceso físico a los locales donde se encuentren ubicados los sistemas de información*	*– Se registran los datos de cada intento de acceso.* *– Los datos se conservan 2 años* *– Está bajo control del responsable de seguridad* *– El responsable de seguridad realiza un informe mensual* *– Existe una excepción: persona física y acceso unipersonal*
Gestión y distribución de soportes y documentos	*– Se identifica el tipo de información que contienen.* *– Se mantiene un inventario* *– Se almacenan con acceso restringido* *– El responsable del fichero autoriza la salida de soportes* *– Se adoptan medidas en caso de desecho de soportes*	*– Existe un registro de entrada y salida de soportes que permite conocer el tipo de soporte o documento, la fecha y hora, el emisor o receptor, el tipo de información, la forma de envío y la persona responsable*	*– Existe un sistema de etiquetado solo comprensible para los usuarios autorizados* *– Se cifran los datos en la distribución de soportes y en los dispositivos portátiles*
Copias de respaldo y recuperación	*– Debe existir un procedimiento de copias de respaldo y recuperación de datos* *– El procedimiento garantiza la reconstrucción de los datos en el estado en que se encontraban en el momento de producirse la pérdida o destrucción* *– Se realiza una copia de respaldo, al menos semanal* *– Verificación semestral de los procedimientos de copia por parte del responsable del fichero* *– Se trabaja sólo con datos reales si se asegura el nivel de seguridad correspondiente al tipo de fichero tratado y se ha hecho una copia.*		*– Debe existir una copia de respaldo y de los procedimientos de recuperación en lugar diferente del que se encuentren los equipos*
Registro de incidencias	*– Se debe registrar tipo de incidencia, momento en que se ha producido, persona que la notifica, persona a la que se comunica y efectos derivados*	*– Se debe registrar la realización de procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y grabados manualmente* *– El responsable del fichero autoriza la ejecución de los procedimientos de recuperación de datos*	
Telecomunicaciones	*– Las medidas de seguridad exigibles a los accesos a través de redes de comunicaciones deben garantizar un nivel de seguridad equivalente a los accesos en modo local*		*– La transmisión de datos a través de redes públicas o de redes inalámbricas debe ser cifrada*

ANEXO

I.M.X. RESUMEN MEDIDAS DE SEGURIDAD RDLOPD - FICHEROS NO AUTOMATIZADOS

	Nivel básico: ficheros o tratamientos de datos de carácter personal
	Nivel medio: ficheros o tratamientos de datos relativos a infracciones administrativas o penales, los que informen de servicios de solvencia patrimonial y crédito, los que sean de Administraciones tributarias, los de prestación de servicios financieros, los de las Entidades Gestoras y Servicios Comunes de la Seguridad Social, los de las mutuas de accidentes de trabajo y los que permitan evaluar la personalidad
	Nivel alto: ficheros o tratamientos de datos relativos a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas y los que contengan datos derivados de actos de violencia de género
Documento de seguridad	*– Implanta la normativa de seguridad concretando el ámbito de aplicación del mismo, las medidas, normas, procedimientos y estándares de seguridad, las funciones y obligaciones del personal, la descripción de los ficheros y de los SSII y los procedimientos de gestión de incidencias, soportes y documentos y copias de seguridad* *– Establece las medidas a adoptar en caso de transporte, reutilización o desecho de soportes y documentos* *– Identifica al encargado del tratamiento y los ficheros afectados y esto se expresa en el DS y en el contrato* *– Se debe mantener actualizado tanto en lo relativo a la organización como a la legislación vigente*
Personal	*– El Documento de Seguridad especifica las funciones y obligaciones de un modo claro y documentado* *– Se difunden entre el personal las normas que les afecten y las consecuencias por incumplimiento*
Registro de incidencias	*Se debe registrar tipo de incidencia, momento en que se ha producido, persona que la notifica, persona a la que se comunica y efectos derivados*
Control y registro de accesos	*– Cada usuario accede únicamente a los datos y recursos necesarios para el desarrollo de sus funciones* *– Existe una relación actualizada de usuarios, perfiles y accesos autorizados* *– Existen mecanismos para controlar los derechos con que se accede a los recursos* *– Existen mecanismos que gestionen la concesión de permisos de acceso sólo por personal autorizado en el Documento de Seguridad*
Gestión de soportes y documentos	*– Se identifica el tipo de información que contienen.* *– Se mantiene un inventario* *– Se almacenan con acceso restringido* *– El responsable del fichero autoriza la salida de soportes* *– Se adoptan medidas en caso de desecho de soportes*
Criterios de archivo	*Se debe garantizar la correcta conservación, localización y consulta de los documentos y posibilitar el ejercicio de los derechos ARCO*
Dispositivos de almacenamiento	*Deben disponer de mecanismos que obstaculicen su apertura*
Custodia de soportes	*Se debe custodiar la documentación cuando no se encuentre en archivada en los dispositivos de almacenamiento*

Responsable de seguridad		*– Es el encargado de coordinar y controlar las medidas de seguridad del documento* *– Esto no supone exoneración de la responsabilidad del responsable del fichero*	
Auditoria		*– Una interna o externa al menos cada 2 años o cuando se realicen cambios sustanciales en los SSII* *– Da lugar a un informe de auditoría sobre la adecuación a las medidas, las deficiencias identificadas y propone medidas correctoras* *– Es analizado por el responsable de seguridad* *– Queda a disposición de la AVPD*	
Almacenamiento de la información			*Archivadores en áreas de acceso protegido con llave u otros sistema equivalente*
Copia o reproducción			*– Sólo personal autorizado en el DS* *– Las copias desechadas se deben destruir*
Acceso a documentación			*– Sólo personal autorizado* *– Existen mecanismos de identificación de accesos* *– Existe un registro de accesos no autorizados*
Traslado de documentación			*Se adoptan medidas para impedir el acceso o manipulación*

II. DATU PERTSONALEN TRATAMENDUARI BURUZKO SUPOSAMENDU ZEHATZEN INGURUKO ERANSKINAK

ERANSKINA

II.I.SZ. IKERKETAKO DATU-TRATAMENDUA

UPV/EHUk ikerketarekin zerikusia duten hiru fitxategi orokor sortu zituen fitxategiei buruzko aitorpena egitean: oinarrizko mailako ikerketa, erdi-mailako ikerketa eta goi-mailako ikerketari dagozkionak, hain zuzen. Aitorpen hori datu pertsonalen fitxategiak sortu, aldatu eta ezabatzeari buruz UPV/EHUren Gobernu Kontseiluak 2007ko otsailaren 8an hartutako erabakiari jarraiki onartu zen (UPV/EHUko idazkari nagusiaren 2007ko otsailaren 28ko erabakiz argitaratua [2007ko apirilaren 11ko EHAA, 69. zk.]).

Alabaina, fitxategi orokor horiez gain, litekeena da UPV/EHUn garatzen diren ikerketa-jardueren ondorioz fitxategi espezifikoak sortu beharra izatea. Ildo horretatik, honako hau xedatzen da:

a) Ikerketa-jarduerarekin loturiko fitxategiak urtebete baino gutxiago iraun behar badu, dagoeneko sorturik dauden fitxategietako batean sartuko da, oinarrizko mailakoan, erdi-mailakoan zein goi-mailakoan.

b) Ikerketa-jarduerarekin loturiko fitxategiak urtebete baino gehiago iraun behar badu:

b.1.– Ikerketa-jarduera horretarako fitxategi espezifiko berri bat sortuko da;

b.2.– Ordurako aitortuta egon daitekeen ikerketako fitxategi espezifikoren batean sartuko da (fitxategiaren aitorpeneko 5.puntuan adierazten diren datuez bestelako daturen bat sartu behar bada, dagoeneko aitortuta dagoen fitxategi espezifikoa aldatu beharko da, ikerketa jarduera berriak bere lekua izan dezan fitxategi horretan).

Ikerketa-jarduera bat egiteko datu pertsonalak erabili behar dituzten ikertzaileek jarduera horri ekin aurretik Ikerketako Errektoreordetzarekin harremanetan jarri beharko dute, arautegi honetako aginduak errespetatzeko jarraibideak ezartze aldera.

ERANSKINA

II.II.SZ. UPV/EHUREN AGINDUZ DATUAK TRATATZEN DITUZTEN KANPOKO ENPRESEK HARTU BEHARREKO KONPROMISOAK

UPV/EHUk, bere beharrei erantzuteko, zerbitzuak ematen dituzten hainbat enpresa kontratatzen ditu. Enpresa horietako batzuk, besteak beste segurtasun-enpresek eta lana bilatzeko lan-poltsak kudeatzen dituztenek,

II. ANEXOS RELATIVOS A SUPUESTOS CONCRETOS DE TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL

ANEXO

II.SC.I TRATAMIENTO DE DATOS EN LA INVESTIGACIÓN

En la Declaración de Ficheros de la UPV/EHU, aprobada en virtud de acuerdo adoptado por el Consejo de Gobierno de la Universidad de 8 de febrero de 2007, para la creación, modificación y supresión de ficheros de datos de carácter personal, publicado por Resolución de 28 de febrero de 2007 del Secretario General de la UPV/EHU (BOPV n.º 69, de 11 de abril de 2007), se crearon los siguientes tres ficheros genéricos relacionados con la Investigación: Investigación nivel básico, Investigación nivel medio e Investigación nivel alto.

No obstante, al margen de los ficheros genéricos, las acciones investigadoras que se desarrollan en la UPV/EHU puede que necesiten la creación de ficheros específicos. En este sentido, se establece que:

a) Si el fichero asociado a la acción investigadora tiene una duración inferior a un año, se integrará en alguno de los ficheros genéricos ya creados de nivel básico, medio o alto.

b) Si el fichero asociado a la acción investigadora tiene una duración superior a un año:

b.1.– Se creará un nuevo fichero específico para esa acción investigadora;

b.2.– Se integrará en alguno de los ficheros de investigación específicos que puedan estar ya declarados (procediendo, si se introduce algún dato diferente respecto a los contenidos en el apartado n.º 5 de la Declaración del fichero, a la modificación del fichero específico ya declarado para que dé cabida a la nueva acción investigadora).

Los investigadores que deseen llevar a cabo una acción investigadora valiéndose de datos de carácter personal, previamente al inicio de una acción investigadora, deberán contactar con el Vicerrectorado de Investigación con el objeto de fijar las pautas a respetar para el cumplimiento de lo establecido en el presente Reglamento.

ANEXO

II.SC.II COMPROMISOS A ASUMIR POR EMPRESAS EXTERNAS QUE REALIZAN TRATAMIENTOS DE DATOS POR CUENTA DE LA UPV/EHU

La UPV/EHU contrata a múltiples empresas proveedoras de servicios con el objeto de dar respuesta a sus propias necesidades. Algunas de estas empresas para cumplir con el cometido que se les ha sido asignado de-

UPV/EHUren fitxategietako datu pertsonalak behar dituzte eman zaien eginkizuna bete ahal izateko. Beraz, enpresa horiek ere datu pertsonalak babesteari buruzko arauak errespetatzen dituztela bermatu beharko du unibertsitateak, haiekin izenpetzen dituen kontratuetan.

UPV/EHUren fitxategietako datu pertsonalak atzitu behar dituzten enpresekin izenpetuko diren kontratuetan -hau da, unibertsitatearen aginduz tratamenduaren arduradun moduan jokatuko duten enpresekin sinatuko direnetan- honako klausula hauek jarriko dira:

Lehenengoa.– Datu pertsonalak atzitzeko beharra

Kontratu honen xede diren eginkizunak betetzeko, UPV/EHUk enpresa esleipendunari datu pertsonalen fitxategiak atzitzen utziko dio, eta enpresa horrek kontratuaren helburuak betetzeko baino ez ditu erabiliko datu horiek.

Bigarrena.– Tratamenduaren arduraduna.

Datu pertsonalak babesteari buruzko abenduaren 13ko 15/1999 Lege Organikoan agindutakoaren arabera, tratamenduaren arduraduna enpresa esleipenduna izango dela ulertzen da; hau da, bera izango da UPV/EHUren aginduz datuak tratatzen dituen pertsona juridikoa. Bestalde, UPV/EHUK, fitxategiaren edo tratamenduaren erantzulea den aldetik, enpresa esleipendunak atzitzen duen informazioak zer helburu eta erabilera izango dituen erabakiko du.

Hirugarrena.– Jarraibideak.

Enpresa esleipendunak UPV/EHUren jarraibideak aintzat hartuz tratatuko ditu datuak, ez bestela. Halaber, datu horiek ez ditu erabiliko kontratu honetan ezarrita ez dauden helburuetarako, eta ez dizkio beste inori jakinaraziko, ezta soilik gordetzeko badira ere.

Laugarrena.– Arautegia betetzea.

Enpresa esleipendunak ezagutzen ditu tratamenduaren arduraduna izateagatik dagozkion betebehar eta errekerimenduak, eta badaki horiek nahitaez errespetatu behar dituela, honako lege eta xedapenen arabera: Datu Pertsonalak Babesteari buruzko 15/1999 Lege Organikoa, abenduaren 13koa; 1720/2007 Errege Dekretua, abenduaren 21ekoa, Datu Pertsonalak Babesteari buruzko abenduaren 13ko 15/1999 Lege Organikoa garatuko duen erregelamendua onartzen duena; eta datu pertsonalak babesteari buruzko beste edozein xedapen aplikagarri.

Bosgarrena.– Segurtasun-neurriak.

Enpresa esleipendunak bere burua behartzen du datuei segurtasun-neurriak ezartzera, tratatuko dituen fitxategien segurtasun-mailaren arabera; hain zuzen ere, honako lege honetan jasota dauden neurriak:1720/2007 Errege Dekretua, abenduaren 21ekoa, Datu Pertsonalak Babesteari buruzko abenduaren 13ko 15/1999 Lege

ben acceder a datos de carácter personal de ficheros de la UPV/EHU; por ejemplo, las empresas de seguridad y las empresas que gestionan las bolsas de búsqueda de empleo. En consecuencia, la Universidad debe asegurarse en el contrato que se suscriba con tales empresas de que éstas van a respetar la normativa en materia de protección de datos de carácter personal.

Las siguientes cláusulas se incluirán en los contratos que se suscriban con empresas que deban a acceder a datos de carácter personal de ficheros de la UPV/EHU, es decir, que actúen como Encargados del tratamiento por cuenta de la Universidad:

Primera.– Necesidad de acceso a los datos de carácter personal.

Para la realización de los servicios objeto del presente contrato la UPV/EHU facilitará a la empresa adjudicataria el acceso a aquellos ficheros de datos de carácter personal que sea necesario, y ésta tratará dichos datos con el fin exclusivo de dar cumplimiento a los objetivos del contrato.

Segunda.– Encargado de tratamiento.

En conformidad lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, queda entendido que la empresa adjudicataria ostenta la condición de Encargado de tratamiento, esto es, persona jurídica que trata los datos por cuenta de la UPV/EHU, quien, como Responsable de fichero o tratamiento, decide la finalidad y el uso de la información a que tiene acceso la empresa adjudicataria.

Tercera.– Instrucciones.

La empresa adjudicataria únicamente tratará los datos conforme a las instrucciones de la UPV/EHU, no los aplicará o utilizará con fin distinto al que figura en el presente contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

Cuarta.– Cumplimiento de la normativa.

La empresa adjudicataria conoce quedar obligada al respeto de los requerimientos y obligaciones que le correspondan en calidad de Encargado de tratamiento según se establece en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como en cualquier otra disposición que en materia de protección de datos le fuera aplicable.

Quinta.– Medidas de seguridad.

La empresa adjudicataria se obliga a aplicar a los datos las medidas de seguridad que se establecen en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica, de 13 de diciembre, de Protección de Datos de Carácter Personal, y que se correspondan con el nivel de

Organikoa garatuko duen erregelamendua onartzen duena. Halaber, kontratu honek iraun bitartean indarrean dauden edo egon daitezkeen segurtasun-neurriak ezartzera behartzen du bere burua.

Seigarrena.– Sekretu profesionala.

Enpresa esleipendunak beti gordeko du isilpean sekretu profesionala, eta UPV/EHUren eskutik jaso dituen datuen konfidentzialtasuna errespetatuko du; beraz, bere burua behartzen du datu horiek hirugarrenei edonola ez erakusteko, ez transferitzeko, ez uzteko edo ez jakinarazteko obligazioa betetzera, baita UPV/EHUrekin duen harremana bukatu ondoren ere. Enpresa esleipendunak bere gain hartzen du kontratu honetan ezarritako obligazioak langileei jakinarazi eta betearazteko konpromisoa, bereziki sekretu profesionala gordetzeari eta segurtasun-neurriak betetzeari buruzko obligazioak.

Zazpigarrena.– Kontratua amaitzea.

Behin zerbitzu-kontratua beteta, enpresa esleipendunak jaso dituen datu pertsonalak suntsituko ditu, edo UPV/EHUri itzuliko dizkio. Beste horrenbeste egingo du edozelako euskarri edo agirirekin ere, halakoek tratamendurako datu pertsonalen bat gordetzen badute, edo jasotako fitxategiei buruzko informazioren bat baldin badute.

ERANSKINA

II.III.SZ. UPV/EHUK ESLEITZEN DIZKIEN EGINKIZUNAK BETETZEAN, UPV/EHUREN ESKU DAUDEN DATUAK ATZITU DITZAKETEN KANPOKO ENPRESEK HARTU BEHARREKO KONPROMISOAK

Datu pertsonalak tratatzea eskatzen ez duten zerbitzuak ematen dituzten enpresetako langileek, UPV/EHUren instalazioetan sartzean, datu pertsonalak gordetzen dituen informazioa atzitu dezakete. Hori gertatzen da, adibidez, garbiketa- eta birziklatze-zerbitzuak ematen dituzten enpresen kasuan.

UPV/EHUk bermatu behar du enpresa horiek eskura duten informazioa ez dutela modu desegokian erabiliko; beraz, horretarako beharrezko neurriak hartuko ditu, eta gutxienez honako klausula hauek jarriko ditu enpresa horiekin izenpetuko dituen kontratuetan:

Lehenengoa.– Datuak tratatzen diren lokaletan sartzea.

Euskal Herriko Unibertsitatean kontratu honen xede diren eginkizunak betetzeko, enpresa esleipenduneko langileek datu-fitxategi pertsonalak eta bestelako dokumentu konfidentzialak tratatzen diren lokaletan sartu beharra daukate.

seguridad de los ficheros a tratar. Así mismo, también queda obligada a aplicar aquellas medidas de seguridad que se encuentren en vigor o puedan estarlo durante la vigencia del presente contrato.

Sexta.– Secreto profesional.

La empresa adjudicataria observará en todo momento el secreto profesional y deber de confidencialidad sobre todos los datos recibidos de la UPV/EHU, obligándose a no revelar, transferir, ceder o comunicar de cualquier forma los datos a terceras personas, obligación que se mantendrá aún finalizada su relación con ésta. La empresa adjudicataria se compromete a comunicar y hacer cumplir a sus empleados las obligaciones establecidas en el presente contrato y, en concreto, las relativas al deber de secreto y medidas de seguridad.

Séptima.– Finalización del contrato.

Una vez cumplida la prestación contractual, la empresa adjudicataria destruirá los datos recibidos o los devolverá a la UPV/EHU, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento o contenga información sobre los ficheros recibidos.

ANEXO

II.SC.III. COMPROMISOS A ASUMIR POR EMPRESAS EXTERNAS QUE EN CUMPLIMIENTO DE LAS FUNCIONES ASIGNADAS POR LA UPV/EHU PUEDAN ENTRAR EN CONTACTO CON DATOS EN MANOS DE LA UPV/EHU

El personal de algunas empresas contratadas por la Universidad para la provisión de servicios que no implican tratamientos de carácter personal, al tener acceso a las instalaciones de la UPV/EHU, pueden tener acceso a información que puede contener datos de carácter personal. Tal circunstancia se da, por ejemplo, en el caso de las empresas de servicios de limpieza y reciclaje contratadas.

La UPV/EHU debe adoptar las medidas necesarias para garantizar que tales empresas no realicen un uso indebido de la información a la que tienen acceso y, por lo tanto, en el contrato a firmar con las mismas se incluirán, como mínimo, las siguientes cláusulas:

Primera.– Acceso a locales de tratamiento.

Para la realización de los servicios objeto del presente contrato en la Universidad del País Vasco / Euskal Herriko Unibertsitatea es necesario que personal de la empresa adjudicataria tenga acceso a locales donde se realizan tratamientos de ficheros con datos de carácter personal así como de otro tipo de documentación de carácter confidencial.

Bigarrena.– Segurtasun-neurriak.

Enpresa esleipenduneko langileek betebeharra daukate sartzen diren lokaletako segurtasun neurriak errespetatzeko, eta langile horiek lokaletan egotearen edo lokaletatik pasatzearen ondorioz ezingo dira hasiera bateko segurtasun-baldintzak eskastu (ate eta leihoak ixtea, alarmen konexioa, eta abar).

Hirugarrena.– Sekretu profesionala.

Enpresa esleipenduneko langileek beti gordeko dute isilpean sekretu profesionala, eta agindu zaizkien eginkizunak betetzean halabeharrez atzitu ditzaketen datuen konfidentzialtasuna errespetatuko dute. Beraz, enpresa esleipenduneko langileek derrigor bete beharko dute datu horiek hirugarrenei edonola ez erakusteko, ez transferitzeko, ez uzteko edo ez jakinarazteko obligazioa, baita UPV/EHUrekin duten harremana bukatu ondoren ere. Enpresa esleipendunak bere gain hartzen du kontratu honetan ezarritako obligazioak langileei jakinarazi eta betearazteko konpromisoa, bereziki sekretu profesionala gorde eta segurtasun-neurriak ezartzeari buruzko obligazioak.

ERANSKINA

II.IV.SZ. KANPOKO ERAKUNDEEK UPV/EHUREN ESKU DAUDEN DATU PERTSONALAK ESKATZEA

Kanpoko erakunde batek UPV/EHUri eskatzen badio bere esku dituen datu pertsonalak uzteko, eta datu horiek hirugarrenei uzteko interesdunen adostasuna behar bada, jarraian adierazitako bideetako bat hautatuko da:

a) Hitzarmena izenpetzea.

Kanpoko erakunderen batek UPV/EHUri eskatzen badio bere esku dituen datu pertsonalak uztea unibertsitateari bere estatutuen arabera interesekoa iruditzen zaion helburu batetarako, datu horiek uzteko hitzarmenaren izapideak egiteari ekingo zaio, aplika daitekeen unibertsitateko araudia errespetatuz.

Hitzarmenari dagozkion izapideak egitean txostenak eskatuko zaizkio DBLO segurtasun-arduradunari eta fitxategiaren edo tratamenduaren pertsona erantzuleari; txosten horiek lotesleak izango dira. Datuak utzi ahal izateko, fitxategi edo tratamenduaren pertsona erantzuleak bere txostenean egiaztatu beharko du eskatzen diren datuen jabeek aurretiaz adostasuna agertu dutela datuak uzteko; adostasun hori agertu ez duten kasuetan, eskatu egin beharko da, arautegi honetako 12. artikuluan ezarritako moduren bat aukeratuz.

Kanpoko erakundearekin izenpetu beharreko hitzarmenak gutxienez honako klausula hauek izan beharko ditu:

Segunda.– Medidas de seguridad.

El personal de la empresa adjudicataria queda obligado a respetar las medidas de seguridad de los locales a los que accede, sin que de su permanencia o paso por ellos pueda derivarse una merma de las condiciones de seguridad originales (cierre de puertas y ventanas, conexión de alarmas, etc.).

Tercera.– Secreto profesional.

El personal de la empresa adjudicataria deberá observar en todo momento el secreto profesional y deber de confidencialidad sobre todos los datos a los que pudiera tener acceso incidentalmente en el cumplimiento de las tareas encomendadas. El personal de la empresa adjudicataria queda obligado a no revelar, transferir, ceder o comunicar de cualquier forma los datos a terceras personas, obligación que se mantendrá aún finalizada su relación con ésta. La empresa adjudicataria se compromete a comunicar y hacer cumplir a sus empleados las obligaciones establecidas en el presente contrato y, en concreto, las relativas al deber de secreto.

ANEXO

II.SC.IV SOLICITUDES DE DATOS DE CARÁCTER PERSONAL EN MANOS DE LA UPV/EHU POR ENTIDADES EXTERNAS

En el caso de que una entidad externa solicite a la UPV/EHU datos de carácter personal en sus manos para cuya cesión a terceros se requiera el consentimiento de los interesados se podrá obrar de una de las dos maneras siguientes:

a) Suscripción de un Convenio.

En el supuesto de que una entidad externa solicite a la UPV/EHU la cesión de datos de carácter personal en sus manos para un fin que la Universidad considere de interés de acuerdo con sus Estatutos, se deberá proceder a la tramitación del correspondiente convenio en función de lo establecido en la normativa universitaria aplicable.

En la tramitación del convenio, se solicitarán informes a la persona Responsable de Seguridad LOPD y a la persona Responsable del fichero o tratamiento, los cuales serán vinculantes. Para que se pueda llevar a cabo la cesión, la persona Responsable del fichero o tratamiento deberá confirmar en su informe que las personas cuyos datos se solicitan han dado previamente el consentimiento para la cesión y, si no lo han hecho, solicitar dicha autorización, siguiendo alguna de las fórmulas establecidas en el artículo 12 del presente Reglamento.

El convenio a suscribir con la entidad externa deberá contener como mínimo las cláusulas siguientes:

Kanpoko erakundeak edo datuen lagapen-hartzaileak berariaz adierazi beharko du datu pertsonalak babesteari buruzko indarreko araudia betetzen duela, eta konpromiso hauek hartuko ditu bere gain:

1.– Uzten zaizkion datuak honako helburu honetarako baino ez erabiltzeko konpromisoa:[adierazi helburu zehatza eta zenbat denbora iraungo duen; hasiera batean une baterako baino ez, eta epe mugatu baterako].

Datuak uztearen helburua errespetatzen ez duen edozein datu-tratamenduren gaineko erantzukizuna lagapen-hartzaileak baino ez du izango, eta lagapen-hartzaile hori eragindako kalteen erantzule gisa agertuko da hirugarrenen aurrean eta unibertsitatearen beraren aurrean.

2.– Berehala datuak tratatzeari utzi eta horiek ezabatzeko konpromisoa, interesdunak datuak ezerezteko eskubidea baliatzen duenean, edo unibertsitateak, egoki deritzolako, lagapen-hartzaileari komunikatzen dionean datuak tratatzeari utziko zaiola.

3.– Datuei honako lege hauetan jasota dauden segurtasun-neurriak ezartzeko konpromisoa: abenduaren 13ko 15/1999 Lege Organikoa, Datu Pertsonalak Babesteari buruzkoa, 9. artikulua; eta 1720/2007 Errege Dekretua, abenduaren 21ekoa, Datu Pertsonalak Babesteari buruzko abenduaren 13ko 15/1999 Lege Organikoa garatuko duen erregelamendua onartzen duena, VIII. Titulua. Konpromiso hori ez errespetatzearen gaineko erantzukizuna lagapen-hartzaileak baino ez du izango, eta lagapen-hartzaile hori eragindako kalteen erantzule gisa agertuko da hirugarrenen aurrean eta unibertsitatearen beraren aurrean.

4.– Uzten zaizkion datuak beste inori ez uzteko konpromisoa.

Fitxategiaren edo tratamenduaren pertsona erantzuleak egiten diren datu-uzteak erregistratuko ditu, etorkizunean datu horiek atzitzeko, zuzentzeko, ezerezteko eta datu horien aurka egiteko eskubideak benetan baliatzen direla bermatzeko. Halaber, egindako datu-uzteak fitxategiaren segurtasun-agiriko sarrera eta irteeren erregistroan agertuko dira.

b) Kanpoko erakundearen informazio-hedapena bere gain hartzea.

Aurreko puntuetan adierazitako prozeduraren salbuespen moduan, kanpoko erakunde batek datuak eskatzen baditu, eta UPV/EHUk pentsatzen badu kanpoko erakundeak emandako informazioa zabaltzen laguntzeko interesa duela (interes horrek zerikusia izan behar du Estatutuen arabera UPV/EHUrenak diren helburuekin), unibertsitateak informazio hori hedatu ahalko du, eta gastuak bere gain hartuko ditu.

Informazio-hedapena antolatzen duen UPV/EHUren unitateak (Errektoregoa, errektoreordetza, gerentzia, ikastegi, institutu edo katedrak) DBLO segurta-

La entidad externa o Cesionaria tendrá que manifestar expresamente que cumple con la normativa de desarrollo vigente en materia de protección de datos de carácter personal, y asumirá los siguientes compromisos:

1.– Tratar los Datos que se le ceden con la finalidad exclusiva de [introducir finalidad con detalle y su duración en el tiempo, en principio para un único momento y durante un plazo de tiempo determinado].

Cualquier tratamiento de los datos que no se ajuste a la finalidad para la que son cedidos, será responsabilidad exclusiva de la Cesionaria, que responderá frente a terceros y frente a la propia Universidad de los daños y perjuicios que pudieren generarse.

2.– Ejercitado el derecho de cancelación de datos por parte de las personas interesadas o cuando la Universidad lo estime oportuno y así lo comunique a la Cesionaria, cesar de inmediato en el tratamiento de los datos y proceder a la supresión de los mismos.

3.– Aplicar a los Datos las medidas de seguridad previstas en el artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como lo dispuesto en el Título VIII del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica, de 13 de diciembre, de Protección de Datos de Carácter Personal. El incumplimiento de este compromiso será responsabilidad exclusiva de la Cesionaria que responderá frente a terceros y frente a la propia Universidad de los daños y perjuicios que pudieran generarse.

4.– No realizar ninguna cesión de los datos que le son cedidos.

La persona Responsable del fichero o tratamiento procederá al registro de las cesiones de datos realizadas, con el fin de garantizar el efectivo futuro ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los interesados. Asimismo, las cesiones realizadas serán reflejadas en el correspondiente Registro de entradas y salidas del Documento de Seguridad del fichero.

b) Asumir la distribución de la información de la entidad externa.

Como salvedad al procedimiento establecido en los apartados anteriores, si se recibe una solicitud de datos por parte de una entidad externa y la UPV/EHU considere de interés colaborar en la divulgación de determinada información facilitada por la entidad externa (interés el cual siempre tendrá que estar relacionado con los fines de la UPV/EHU según sus Estatutos), la Universidad podrá llevar a cabo dicha distribución y correr con los gastos.

La unidad organizativa de la UPV/EHU implicada (Rectorado, Vicerrectorados, Gerencia, Centros, Institutos y Cátedras), tras la correspondiente aprobación de

sun-arduradunari eskatuko dio dagokion baimena, unitateko arduradun nagusiak informazioa hedatzeko ekimen horri adostasuna eman ostean. DBLO segurtasun-arduradunak baimen hori idatziz eman ostean, unitate antolatzaileak bere gain hartuko du kanpoko erakundeak emandako informazioa hedatzeko ardura. Informazio horrek aurretik unibertsitatearen aurkezpen-idazkia izango du, eta bertan informazio hori bidaltzea justifikatuko da.

Informazioa hedatzeko lehenetsitako bidea posta elektronikoa izango da. Salbuespen moduan, ohiko posta erabiliko da. Horretarako, DBLO segurtasun-arduradunari egindako eskaeran behar bezala justifikatuko da ohiko posta erabiltzeko arrazoia.

Halaber, unibertsitatearen web-orrian gune batzuk gorde ahalko dira bertan unibertsitateko kideentzat interesgarria den informazioa jartzeko, informazio horrek unibertsitatearekin zerikusi zuzena izan ez arren; bestalde, informazio hori jartzeko ezarritako prozedura errespetatuko da.

ERANSKINA

II.V.SZ. AGINTARI JUDIZIAL, POLIZIAL ETA ADMINISTRATIBOEN DATU-ESKAERA

1.– UPV/EHUren esku dauden fitxategietako datu pertsonalei buruzko informazioa, ikasleak, langileak edo hirugarrenak ukitzen dituena, agintari judizial, polizial edo administratiboei jakinaraziko zaie, legeak ezarritako prozedurari eta jarraian adierazitako arauei jarraiki. Datu pertsonalei buruzko informazio-eskaerak arrazoitzen ez badira, ez dira onartuko. Agintari judizial, polizial edo administratiboei egindako datu-uzteak DBLO segurtasun-arduradunak eta fitxategiaren edo tratamenduaren pertsona erantzuleak ikuskatuko ditu.

2.– Agintari judizial, polizial eta administratiboek datuak uzteko eskaera egiten duten momentutik, unibertsitateko Lege Zerbitzuarekin harremanetan jarri beharko da. Ez da inolako informaziorik bidaliko, Lege Zerbitzuak aurretiaz bere oniritzia ematen ez badu. Lege Zerbitzua arduratuko da fitxategiaren edo tratamenduaren pertsona erantzulearekin eta DBLO segurtasun-arduradunarekin harremanetan jartzeaz. Ez da inolako daturik emango, aurretiaz Lege Zerbitzuak bere oniritzia ematen ez badu.

3.– Agintari judizialen eskaerei erantzungo zaie epailearen bitartekotzarekin eginak diren neurrian. Gobernu-organoek prozesu judizialak prestatu edo osatzeko jarduerekin lotura zuzena duten informazio-eskaerak egiten dituztenean, horiei erantzungo zaie, idatziz argi jasota geratzen denean zein den zehazki eskaera egin duen gobernu-organo hori.

4.– Agintari polizialen eskaerei dagokienez, poliziaren fitxategiak arautzen dituen artikulu berezia dago

la iniciativa por su máxima persona responsable, solicitará el permiso correspondiente a la persona Responsable de Seguridad LOPD. Una vez de haber recibido la autorización por escrito de la persona Responsable de Seguridad LOPD, la unidad organizativa interesada se encargará del envío de la información facilitada por la entidad externa, la cual irá introducida por un escrito de presentación de la Universidad que justifique el interés de dicho envío.

El medio prioritario de distribución será el correo electrónico. Tan sólo en supuestos excepcionales, debidamente justificados en la solicitud que se realice a la persona Responsable de Seguridad LOPD, se procederá al envío por correo postal.

Asimismo, se podrán habilitar en la web de la Universidad lugares en los que se pueda colocar información no directamente relacionada con la Universidad pero de interés para la comunidad universitaria, conforme al procedimiento que se establezca al efecto.

ANEXO

II.SC.V SOLICITUDES DE DATOS DE AUTORIDADES JUDICIALES, POLICIALES Y ADMINISTRATIVAS

1.– La información sobre datos de carácter personal obrantes en ficheros de la UPV/EHU que puede afectar a alumnado, personal o terceros, será comunicada a autoridades judiciales, policiales y administrativas, con sujeción al procedimiento legalmente establecido y a las reglas que se exponen a continuación. No se atenderán peticiones de información sobre datos de carácter personal no motivadas. La cesión de datos a autoridades judiciales, policiales y administrativos será supervisada por la persona Responsable del fichero o tratamiento y la persona Responsable de Seguridad LOPD.

2.– En el momento en que se obtenga una solicitud de de datos por parte de autoridades judiciales, policiales y administrativas, se contactará con el Servicio Jurídico de la Universidad. No se procederá a la remisión de ninguna información sin el previo visto bueno del Servicio Jurídico. El Servicio Jurídico se encargará de contactar con la persona Responsable del fichero o tratamiento y la persona Responsable de Seguridad LOPD. No se procederá a la entrega de ningún dato sin el previo visto bueno del Servicio Jurídico.

3.– Las solicitudes realizadas por autoridades judiciales, se facilitarán en la medida en que sean solicitadas mediando la intervención del juez. Las informaciones solicitadas por órganos gubernativos directamente relacionados con actuaciones preparatorias o complementarias de procesos judiciales, serán facilitadas cuando conste claramente la intervención de órgano judicial concreto.

4.– En relación con las solicitudes realizadas por las autoridades policiales, los ficheros policiales tienen una

DBLOn; 22. artikulua, hain zuzen ere. Artikulu horren arabera, interesdunen adostasunik gabe segurtasunerako poliziaren indarrek eta kidegoek polizia-xedeetarako baino ez dituzte bildu edota tratatuko irakaskuntzarako zentro publikoek beren esku dituzten datu pertsonalak; bilketa eta tratamendu hori mugatuko da kasu haueta-ra: segurtasun publikoa benetan arriskuan jartzen duten egoerak prebenitzera eta arau-hauste penalak zigortzera. Beraz, eginkizun horrekin zerikusirik duten datuak biltzeko fitxategi espezifikoak ezarriko dira, eta bertan gorde beharko dira datuak, fidagarritasun-mailaren arabera sailkaturik. Artikulu horren arabera, segurtasunerako poliziaren indar eta kidegoek baimena dute datuak lortu eta tratatzeko; horretarako, datuak uzteko eskaeraren jatorria adierazi beharko da, eta baldintza hauek bete:

a) Behar bezala egiaztatu beharko da datuak biltzea beharrezkoa dela segurtasun publikorako benetakoa eta larria den arrisku bat prebenitzeko, edo arau-hauste penalak zigortzeko.

b) Eskaera zehatza eta espezifikoa egin beharko da; izan ere, lehen adierazitakoa eta datu-eskaera masiboa ez dira bateragarriak.

c) Eskaera behar bezala arrazoitu beharko da, eta adierazi diren kasuekin lotura duela egiaztatu beharko da.

d) Datuak ezereztu egin beharko dira beharrezkoak izateari uzten diotenean datu horiek biltzeko arrazoia izan zen miaketarako, DBLOren 22.4. artikuluak ezarritakoa betez.

5.– Agintari administratiboek eskatutako datuak emango dira, baldin eta:

a) Eskaera Zerga Ikuskaritzak, lurralde historikoetako foru ogasunek, edo toki ogasunen zerga-bilketarako bulegoek aurkezten badute eta eskatutako informazioak garrantzia badu zergei dagokienez, honako hauek ezarritakoari jarraiki: Zergari buruzko Lege Orokorra, 111 eta 112. artikuluak; zergen ikuskaritzari buruzko arautegi orokorraren 37. artikulua; dagokion foru-araudia, edo une bakoitzean indarrean dagoen araudia.

b) Eskaera Gizarte Segurantzaren Institutu Nazionalak edo bere agentziaren batek egiten badu, dituen eskumenak erabiliz.

c) Eskaera dagokion lan-agintaritzak egiten badu, dituen eskumenak erabiliz.

d) Funtzio publiko estatistikoari buruzko maiatzaren 12ko 12/1989 Legean eta Euskal Autonomia Erkidegoko Estatistikari buruzko apirilaren 23ko 4/1986 Legean oinarriturik egiten bada eskaera, horrelako ikerketak egiteko.

e) Lege baten arabera datuak derrigor utzi behar badira.

regulación especial contenida dentro del artículo 22 de la LOPD y en base a ella, la recogida y tratamiento para fines policiales de datos de carácter personal manejados por centros públicos de enseñanza, por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad. Este artículo habilita a las Fuerzas y Cuerpos de Seguridad para la obtención y tratamiento de los datos, lo que llevará aparejada la procedencia de la cesión instada, siempre y cuando se cumplan las siguientes condiciones:

a) que quede debidamente acreditado que la obtención de los datos resulta necesaria para la prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales;

b) que se trate de una petición concreta y específica, al no ser compatible con lo señalado el ejercicio de solicitudes masivas de datos;

c) que la petición se efectúe con la debida motivación, que acredite su relación con lo supuestos que se han expuesto;

d) que los datos sean cancelados cuando dejen de ser necesarios para las averiguaciones que motivaron su almacenamiento, en cumplimiento del artículo 22.4 de la LOPD.

5.– Se facilitarán los datos solicitados por autoridades administrativas cuando:

a) la solicitud haya sido presentada por la Inspección Tributaria, la Agencia Estatal Tributaria, las Haciendas Forales de los Territorios Históricos o las Oficinas Recaudatorias de las Haciendas Locales, en virtud de lo establecido en los artículos 111 y 112 de la Ley General Tributaria, el artículo 37 del Reglamento General de Inspección de Tributos, y la correspondiente normativa foral, o normativa vigente en cada momento y siempre que la información solicitada tenga trascendencia tributaria;

b) la solicitud sea presentada por el Instituto Nacional de la Seguridad Social o cualquiera de sus Agencias, en el ejercicio de las competencias que le son propias;

c) la solicitud sea presentada por la autoridad laboral correspondiente en el uso de las competencias que le son propias;

d) la solicitud de datos se presente basada en la Ley 12/1989, de 12 de mayo, sobre Función Pública Estadística y la Ley 4/1986, de 23 de abril, de Estadística de la Comunidad Autónoma del País Vasco, para la elaboración de estudios de este carácter;

e) siempre que las cesiones sean obligatorias en virtud de una ley.

ERANSKINA

II.VI.SZ. UPV/EHUK KANPOKO ERAKUNDEEI ZERBITZUAK EMATEA

Enpresa/erakundeekin izenpetzen diren hitzarmen/kontratuetan honako klausula hauek jarriko dira, unibertsitatea, hirugarrenen enkarguz, datu pertsonalen tratamenduaren arduraduna baldin bada.

Lehenengoa.– Datu pertsonalak atzitzeko beharra.

Hitzarmen/kontratu honen xede diren zerbitzuak emateko, (adierazi unibertsitateak zein erakunde edo enpresarekin izenpetzen duen hitzarmen edo kontratua)k UPV/EHUri behar dituen datu pertsonalen fitxategiak atzitzen utziko dio, eta unibertsitate horrek hitzarmen/kontratuaren helburuak betetzeko baino ez ditu erabiliko datu horiek.

Bigarrena.– Tratamenduaren arduraduna.

Datu pertsonalak babesteari buruzko abenduaren 13ko 15/1999 Lege Organikoan agindutakoaren arabera, UPV/EHU tratamenduaren arduraduna izango dela ulertzen da; hau da, bera izango da (adierazi unibertsitateak zein erakunde edo enpresarekin izenpetzen duen hitzarmen edo kontratua)ren aginduz datuak tratatzen dituen pertsona juridikoa. Bestalde, (adierazi unibertsitateak zein erakunde edo enpresarekin izenpetzen duen hitzarmen edo kontratua)k, fitxategiaren erantzulea den aldetik, UPV/EHUK atzitzen duen informazioak zer helburu eta erabilera izango dituen erabakiko du.

Hirugarrena.– Jarraibideak.

UPV/EHUk (adierazi unibertsitateak zein erakunde edo enpresarekin izenpetzen duen hitzarmen edo kontratua)ren jarraibideak aintzat hartuz tratatuko ditu datuak, ez bestela. Halaber, datu horiek ez ditu erabiliko hitzarmen/kontratu honetan ezarrita ez dauden helburuetarako, eta ez dizkio beste inori jakinaraziko, ezta soilik gordetzeko badira ere.

Laugarrena.– Arautegia betetzea.

(adierazi unibertsitateak zein erakunde edo enpresarekin izenpetzen duen hitzarmen edo kontratua) k ezagutzen ditu fitxategiaren edo tratamenduaren erantzulea izateagatik dagozkion betebehar eta errekerimenduak, eta badaki horiek nahitaez errespetatu behar dituela, honako lege eta xedapenen arabera: Datu Pertsonalak Babesteari buruzko 15/1999 Lege Organikoa, abenduaren 13koa; 1720/2007 Errege Dekretua, abenduaren 21ekoa, Datu Pertsonalak Babesteari buruzko abenduaren 13ko 15/1999 Lege Organikoa garatuko duen erregelamendua onartzen duena; datu pertsonalak babesteari buruzko beste edozein xedapen aplikagarri, bereziki Datuak Babesteko Euskal Bulegoari fitxategiak aitortzeko betebeharra ezartzen duena, eta aplikagarriak diren bestelako xedapenak.

ANEXO

II.SC.VI. PRESTACIÓN DE SERVICIOS POR PARTE DE LA UPV/EHU A ENTIDADES EXTERNAS

Las siguientes cláusulas se incluirán en los convenios/contratos que se suscriban con empresas/entidades cuando la Universidad actúe como Encargada del tratamiento de datos de carácter personal por cuenta de terceros.

Primera.– Necesidad de acceso a los datos de carácter personal.

Para la realización de los servicios objeto del presente convenio/contrato la (entidad o empresa con quien se subscribe el convenio o contrato), facilitará a la UPV/EHU el acceso a aquellos ficheros de datos de carácter personal que sea necesario, y esta tratará dichos datos con el fin exclusivo de dar cumplimiento a los objetivos del convenio/contrato.

Segunda.– Encargado de tratamiento.

En conformidad lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal con, queda entendido que la UPV/EHU ostenta la condición de Encargado de tratamiento, esto es, la persona jurídica que trata los datos por cuenta de (la entidad o empresa con quien se subscribe el convenio o contrato), quien, como responsable de fichero, decide la finalidad y el uso de la información a que tiene acceso la UPV/EHU.

Tercera.– Instrucciones.

La UPV/EHU únicamente tratará los datos conforme a las instrucciones que de (la entidad o empresa con quien se subscribe el convenio o contrato), no los aplicará o utilizará con fin distinto al que figura en el presente convenio/contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

Cuarta.– Cumplimiento de la normativa.

La (entidad o empresa con quien se subscribe el convenio o contrato), conoce quedar obligada al respeto de los requerimientos y obligaciones que le correspondan en calidad de Responsable de fichero o tratamiento según se establece en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como en cualquier otra disposición que en materia de protección de datos le fuera aplicable, en particular, de la obligación de tener declarados los ficheros ante la Agencia de Protección de Datos correspondiente, así como en cualquier otra disposición que en materia de protección de datos le fuera aplicable.

Bosgarrena.– Segurtasun-neurriak.

UPV/EHUk bere burua behartzen du datuei segurtasun-neurriak ezartzera, tratatuko dituen fitxategien segurtasun-mailaren arabera; hain zuzen ere, honako lege honetan jasota dauden neurriak:1720/2007 Errege Dekretua, abenduaren 21ekoa, Datu Pertsonalak Babesteari buruzko abenduaren 13ko 15/1999 Lege Organikoa garatuko duen erregelamendua onartzen duena. Halaber, kontratu honek iraun bitartean indarrean dauden edo egon daitezkeen segurtasun-neurriak ezartzera behartzen du bere burua.

Seigarrena.– Sekretu profesionala.

UPV/EHUK beti gordeko du isilpean sekretu profesionala, eta (adierazi unibertsitateak zein erakunde edo enpresarekin izenpetzen duen hitzarmen edo kontratua)ren eskutik jaso dituen datuen konfidentzialtasuna errespetatuko du; beraz, bere burua behartzen du datu horiek hirugarrenei edonola ez erakusteko, ez transferitzeko, ez uzteko edo ez jakinarazteko obligazioa betetzera, baita (adierazi unibertsitateak zein erakunde edo enpresarekin izenpetzen duen hitzarmen edo kontratua)rekin duen harremana bukatu ondoren ere. UPV/EHUk bere gain hartzen du kontratu honetan ezarritako obligazioak langileei jakinarazi eta betearazteko konpromisoa, bereziki sekretu profesionala gorde eta segurtasun-neurriak betetzeari buruzko obligazioak.

Zazpigarrena.– Kontratua amaitzea.

Behin zerbitzu-kontratua beteta, UPV/EHUk jaso dituen datu pertsonalak suntsituko ditu, edo (adierazi unibertsitateak zein erakunde edo enpresarekin izenpetzen duen hitzarmen edo kontratua)ri itzuliko dizkio. Beste horrenbeste egingo du edozelako euskarri edo agirirekin ere, halakoek tratamendurako datu pertsonalen bat gordetzen badute, edo jasotako fitxategiei buruzko informazioren bat baldin badute.

ERANSKINA

II.VII.SZ. AZTERKETAN NOTAK ARGITARATZEA

Azterketan notak iragarki-oholetan argitaratuko dira, eta ikaslea identifikatzeko NAN zenbakia baino ez da erabiliko.

Azterketen notak argitara emateko helburua bete dadin eta ikasleek beren eskubideak baliatu ahal izan ditzaten, nahikoa denbora utziko da noten zerrendak kendu aurretik, baina denbora horrek ez du inoiz hilabetea gaindituko.

Zerrenda horiek klausula bat izango dute, honako hau adieraziko duena:

Zerrenda honek datu pertsonalak ditu eta datuak babesteari buruzko gaur egungo arautegia betetzen du; bere helburu bakarra ebaluazio-prozesu hau argitara ematea da. Ez da jendearen eskurako iturria eta ezin da zerrenda osoaren nahiz zati baten kopiarik egin; halaber, informazioa berreskuratzeko inolako sistemaren

Quinta.– Medidas de seguridad.

La UPV/EHU se obliga a aplicar a los datos las medidas de seguridad que se establecen en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica, de 13 de diciembre, de Protección de Datos de Carácter Personal, y que se correspondan con el nivel de seguridad de los ficheros a tratar. Así mismo, también queda obligada a aplicar aquellas medidas de seguridad que se encuentren en vigor o puedan estarlo durante la vigencia del presente contrato.

Sexta.– Secreto profesional.

La UPV/EHU observará en todo momento el deber de confidencialidad sobre todos los datos recibidos de (la entidad o empresa con quien se subscribe el convenio o contrato), obligándose a no revelar, transferir, ceder o comunicar de cualquier forma los datos a terceras personas, obligación que se mantendrá aún finalizada su relación con ésta. La UPV/EHU se compromete a comunicar y hacer cumplir a sus empleados las obligaciones establecidas en el presente convenio/contrato y, en concreto, las relativas al deber de secreto y medidas de seguridad.

Séptima.– Finalización del contrato.

Una vez cumplida la prestación contractual, la UPV/EHU destruirá los datos recibidos o los devolverá a (la entidad o empresa con quien se subscribe el convenio o contrato), al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento o contenga información sobre los ficheros recibidos.

ANEXO

II.SC.VII PUBLICIDAD DE NOTAS DE EXÁMENES

La publicación de notas de exámenes se llevará a cabo en los tablones de anuncios mediante la identificación del alumnado únicamente con su DNI.

Los listados para dar publicidad de notas de exámenes se mantendrán durante el tiempo necesario para cumplir su finalidad de publicidad, que nunca podrá ser superior a un mes, y permitir el ejercicio de los derechos del alumnado.

Los mencionados listados incorporarán una cláusula advirtiendo lo siguiente:

«Este listado contiene datos de carácter personal, se ajusta a la normativa actual en materia de protección de datos y su única finalidad es la dar publicidad al presente proceso de evaluación. No constituye fuente de acceso público y no podrá ser reproducido ni en todo ni en parte, ni transmitido ni registrado por ningún sistema

bitartez ezingo da zerrenda transmititu, ezta erregistratu ere, interesdunek horretarako adostasunik agertzen ez badute.

Web orrietan azterketen notak argitaratzeko, sarbide-gakoa eskatuko duen sarbide-kontrola ezarriko da; hala, interesdunak baino ezingo du egin kontsulta.

ERANSKINA

II.VIII.SZ. LEHIAKETA BIDEZKO PROZESUAK

Lehiaketa bidezko prozesuetan argitara emango diren behin-behineko eta behin betiko zerrendetan datu pertsonal gutxi agertuko dira, zabalkunde printzipioak betetzeko beharrezkoak direnak baino ez (izena, abizenak eta NAN zenbakia), argitara emateko modua edozein dela ere (iragarki-ohola, web-orria...). Zerrenda horiek dagokien prozesua amaitu arte egongo dira ikusgai eta, era berean, erreklamazioak edo errekurtsoak jartzeko beharrezkoa izan daitekeen denbora guztian.

Zenbait prozesutan, eskumena daukan organoak NAN zenbakia baizik ez argitaratzea erabaki dezake.

Unibertsitatekoak diren lehiaketa bidezko prozesuetan, adibidez beka-deialdietan, poltsa eta laguntzen deialdietan eta praktiketan, izen-abizenak jartzearekin nahikoa izango da.

Zerrenda horiek klausula bat izango dute, honako hau adieraziko duena:

Zerrenda honek datu pertsonalak ditu eta datuak babesteari buruzko gaur egungo arautegia betetzen du; bere helburu bakarra ebaluazio-prozesu hau argitara ematea da. Ez da jendearen eskurako iturria eta ezin da zerrenda osoaren nahiz zati baten kopiarik egin; halaber, informazioa berreskuratzeko inolako sistemaren bitartez ezingo da zerrenda transmititu, ezta erregistratu ere, interesdunek horretarako adostasunik agertzen ez badute.

ERANSKINA

II.IX.SZ. IRAKASLEEK IKASLEEN DATUAK ESKURATZEA

Ikasturte bakoitzaren hasieran irakasleek jakin eta eskuratu behar dituzten ikasleei buruzko datu pertsonalak (argazkia barne) akademi gestiorako sistema informatikoaren bidez lortu ahal izango dituzte.

Beraz, orain arteko sistema tradizionalak ez du balio, eta ezingo dira erabili ikasturte bakoitzaren hasieran irakasleek eskatzen zituzten eskuz egindako fitxak.

Matrikula egitean ikasleari adieraziko zaio zertarako erabiliko den bere argazkia.

de recuperación de información, sin el consentimiento de los propios afectados.»

La publicidad de notas de exámenes del alumnado en páginas web sólo se realizará con un control de acceso mediante clave que impida su consulta a personas distintas a la persona interesada.

ANEXO

II.SC.VIII PROCESOS DE CONCURRENCIA COMPETITIVA

La publicidad de los listados provisionales y definitivos en los procesos de concurrencia competitiva con independencia del medio en que se hagan públicos (tablón de anuncios, página web,…), contendrán los datos de carácter personal mínimos necesarios para cumplir el principio de publicidad (nombre, apellidos y DNI) y se mantendrán hasta la finalización del correspondiente proceso y durante el tiempo adicional necesario para el ejercicio de las reclamaciones o recursos.

En determinados procesos, el órgano competente podrá optar por restringir la publicación de datos de carácter personal al DNI.

En los procesos de concurrencia competitiva de carácter universitario tales como convocatorias de becas, bolsas y ayudas, y prácticas, bastará con el nombre y apellidos.

Los mencionados listados incorporarán una cláusula advirtiendo que:

«Este listado contiene datos de carácter personal, se ajusta a la normativa actual en materia de protección de datos y su única finalidad es la dar publicidad al presente proceso de selección. No constituye fuente de acceso público y no podrá ser reproducido ni en todo ni en parte, ni transmitido ni registrado por ningún sistema de recuperación de información, sin el consentimiento de los propios afectados o afectadas.»

ANEXO

II.SC.IX OBTENCIÓN DE DATOS DEL ALUMNADO POR PARTE DEL PROFESORADO

Al inicio de cada curso los datos de carácter personal que el profesorado necesita saber de su alumnado, incluida su fotografía, estarán disponibles a través del sistema informático de gestión académica de la Universidad.

Por lo tanto, no se permite el sistema tradicional de fichas manuales que hasta la fecha eran solicitadas por el profesorado al inicio de cada curso.

En el momento de hacer la matrícula se informará al alumnado de la finalidad y uso que se va a realizar de su fotografía.

ERANSKINA

II.X.SZ. UNIBERTSITATEAREN WEB ORRIA

1.– Sarrera libreko UPV/EHUren web orriek ezin dituzte datu pertsonalak izan, ez badituzte baldintza hauek betetzen:

a) UPV/EHUk aitortutako fitxategietakoak izatea.

b) Datuen jabeek titularrari adostasuna agertzea, web orrian erakusten diren datuak argitaratzeko.

2.– Ez dira argitaratuko ikasle-taldeen zerrendak (irakasgaietako taldeak, praktiketakoak eta abar), kasu hauetan izan ezik:

a) Autentifikazio-prozesu bati esker interesdunak baino sartu ezin direnean.

b) Interesdunek zerrendak argitaratzeko prozedurarekiko adostasuna agertu dutenean.

3.– Datu pertsonalak helburu zehatz batekin biltzen direnean, interesdunari arautegi honetako 7.1. artikuluan aipatzen den informazioa eman beharko zaio.

4.– UPV/EHUren web orriek zorrotz bete behar dute unibertsitatearen pribatutasun-politika. Politika hori unibertsitatearen interneteko atarian argitara ematen da, «Lege oharra» izeneko atalean, «Datu pertsonalak babesteko politika» izenburupean.

1) Euskal Herriko Unibertsitateak web guneko erabiltzaileei jakinarazten die web gunea erabiltzearen ondorioz emandako datu pertsonalekin artxibo automatizatu bat egin dezakeela; betiere, datuak babesteko arautegiari jarraiki.

2) Erabiltzaileek bermatzen dute web gunea erabiltzerakoan eman dituzten datuak egiazkoak direla. Alde horretatik, erabiltzaileen ardura da datuak eguneratuta edukitzea, unean uneko errealitatearekin bat etor daitezen. Emandako datuen ondorioz gezurrezko adierazpenak edo adierazpen okerrak egiten badira eta informazio horrek kalteak eragiten baditu, erantzuleak erabiltzaileak izango dira.

3) Datu Pertsonalak Babesteko abenduaren 13ko 15/1999 Lege Organikoak zehaztutakoari jarraiki, datu pertsonalak bildu eta datu-fitxategi batean gordeko dira; fitxategi horren erantzulea Euskal Herriko Unibertsitateko gerentzia da.

ANEXO

II.SC.X PÁGINA WEB CORPORATIVA

1.– Las páginas web de la UPV/EHU de acceso libre no deben contener datos de carácter personal salvo que se cumplan las siguientes condiciones:

a) Correspondan a ficheros declarados por la UPV/EHU.

b) Y el titular posea consentimiento expreso para su publicación otorgado por las personas cuyos datos son mostrados en la página.

2.– No se publicarán listas de grupos de alumnado (de asignaturas, de prácticas, etc.) salvo en los siguientes supuestos:

a) Sólo puedan acceder las personas interesadas mediante un proceso de autenticación.

b) Las personas afectadas hayan dado su consentimiento al procedimiento de publicación de listas.

3.– Cuando se recaben datos de carácter personal con una finalidad determinada, debe informarse a la persona interesada de los extremos mencionados en el artículo 7.1 del presente Reglamento.

4.– Las páginas web de la UPV/EHU deben cumplir rigurosamente, en lo que les afecte, la política de privacidad de la Universidad, la cual se publicita en el portal corporativo en el apartado relativo a «Información Legal» bajo el epígrafe «Política de protección de datos de carácter personal»:

1) La Universidad del País Vasco / Euskal Herriko Unibertsitatea pone en conocimiento de los usuarios de este sitio que podrá crear un archivo automatizado con los datos de carácter personal que sean facilitados a la misma como consecuencia de la utilización del presente sitio web y en estricto cumplimiento con lo preceptuado en la normativa en materia de protección de datos de carácter personal.

2) Los usuarios garantizan la veracidad y autenticidad de las informaciones y datos que comuniquen en virtud de la utilización de este sitio web. En este sentido, será de obligación de los usuarios el mantener actualizados las informaciones y datos de forma tal que correspondan a la realidad en cada momento. Cualquier manifestación falsa o inexacta que se produzca como consecuencia de las informaciones y datos manifestados así como los perjuicios que tal información pudiera causar será responsabilidad de los usuarios.

3) En cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se informa que los datos de carácter personal serán recopilados y archivados en un fichero de datos cuyo responsable es la Gerencia de la Universidad del País Vasco / Euskal Herriko Unibertsitatea.

4) Erabiltzaileek bildutako eta artxibatutako haien datu pertsonalak atzitzeko, zuzentzeko, ezerezteko eta datuen aurka egiteko eskubidea daukate. Horretarako, idatzi bat bidali behar diote Euskal Herriko Unibertsitateko DBLO segurtasun-arduradunari. Eskubide horiek erabiltzeak ez du eraginik izango web gunerako sarbidean, ezta erabiltzaileen harpidetzan ere.

5) Erregistratutako datuak erabil daitezke datu-bilketaren xede diren ekintzetarako eta, gainera, estatistikak egiteko, informazio zientifikoa bidaltzeko, intzidentziak kudeatzeko eta merkatu-azterketak egiteko.

6) Erabiltzaileek emandako datu pertsonalak hirugarrenei emango zaizkie, bakarrik, aipatu helburuekin eta, betiere, Datu Pertsonalak Babesteko 15/1999 Lege Organikoaren 11. eta 21. artikuluei jarraiki; alde horretatik, interesdunen baimena hala dagokionean bakarrik eskatuko da.

7) Euskal Herriko Unibertsitateari datu pertsonalak emateak esan nahi du erabiltzaileak ados daudela datu horiek Euskal Herriko Unibertsitateak erabiltzearekin.

8) Euskal Herriko Unibertsitateak datu pertsonalak ezkutuan gordetzeko konpromisoa hartzen du bere gain; halaber, neurri teknikoak eta antolakuntza-neurriak hartzeko asmoa agertzen du, datu horiek seguru gorde eta datuak aldatu, galdu edo baimenik gabe eskuratzea ekiditeko, kontuan hartuta teknologiaren gaur egungo egoera, bildutako datuen izaera eta datuen arriskuak, bai gizakiek eta ingurune fisiko eta naturalak eragin ditzaketenak.

ERANSKINA

II.XI.SZ. WEB DIREKTORIOA

UPV/EHUren web orriko langileak atalean unibertsitatearen zerbitzurako lan egiten duten guztien identifikazioa eta haiekin harremanetan jartzeko datuak aurkitzen dira. Unibertsitateko kideen arteko komunikazioa bermatzeko, kontsultak egiteko aukera ematen da, baina horretarako kontsulta-egileak kautotu egin behar du. Hala eginez gero, identifikazio-datu guztiak eta harremanetan jartzekoak ikus daitezke; bestalde, unibertsitateaz kanpoko edonork langile horien datuak kontsultatzea galarazteko, kautotze-sistemaren bitartez kanpokoei ezkutatu nahi zaizkien identifikaziorako eta harremanetarako datuak ez erakusteko aukera dago.

4) Los usuarios podrán ejercitar, en cualquier momento, los derechos de acceso, rectificación, cancelación y oposición de sus datos recopilados y archivados. El ejercicio de estos derechos deberá efectuarse mediante comunicación escrita dirigida a la persona Responsable de seguridad LOPD de la Universidad del País Vasco / Euskal Herriko Unibertsitatea. El ejercicio de estos derechos no afectara en modo alguno al acceso a la página web ni, en su caso, a la condición de abonado del usuario.

5) Los datos registrados podrán ser utilizados con la finalidad de efectuar estadísticas, la remisión de información científica, la gestión de incidencias o la realización de estudios de mercado, además de para las que expresamente se hayan recabado los datos.

6) En su caso, los datos de carácter personal facilitados por los usuarios podrán ser comunicados a un tercero sólo para el cumplimiento de los fines señalados anteriormente, ajustándose a lo establecido en los artículos 11 y 21 de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, recabándose, en todo caso, el consentimiento de los interesados cuando este sea necesario.

7) Al facilitar los datos de carácter personal a la Universidad del País Vasco / Euskal Herriko Unibertsitatea, los usuarios declaran aceptar plenamente y sin reservas el tratamiento de los mismos por parte de la Universidad del País Vasco / Euskal Herriko Unibertsitatea.

8) La Universidad del País Vasco / Euskal Herriko Unibertsitatea se compromete a cumplir con la obligación de guardar secreto respecto de los datos de carácter personal objeto de tratamiento y declara su intención de poner en práctica las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

ANEXO

II.SC.XI DIRECTORIO WEB

En el Directorio web de la UPV/EHU se encuentran los datos de identificación y contacto de todo el personal al servicio de la Universidad. Para garantizar, por una parte, la posibilidad de comunicación entre los distintos miembros de la comunidad universitaria se posibilita efectuar las consultas autenticándose la persona que las realiza, siendo visibles en ese supuesto todos los datos de identificación y contacto del personal; por otra parte, para permitir el derecho de las personas de que sus datos no sean consultados por cualquier persona ajena a la comunidad universitaria se permite a través del propio sistema de autenticación ocultar hacía el exterior los datos de identificación y contacto que se quieran restringir.

ERANSKINA

II.XII.SZ. LAN-BALDINTZAK ZAINDU ETA BABESTEKO DATU-UZTEA

Langileen ordezkari diren organoek lan-baldintzak zaindu eta babesteko duten eginkizuna modu egokian bete dezaten, ez dago UPV/EHUren zerbitzurako lan egiten duten langileei buruzko datuak masiboki uzteko beharrik.

Alabaina, arazo zehatz bat sortu duen pertsona partikular bat zaindu edo kontrolatu behar denean, pertsona horri buruzko datu espezifikoa eman ahalko da.

Gainerako kasuetan, kontrolatzeko eginkizuna erabat beteko da informazioa modu agregatuan utziz; edo, bestela, informazioa behar bezala bereizirik utziz. Hau da, datuek ezingo dituzte aipatu identifikatutako pertsonak edo identifikagarriak direnak, eta era berean, pertsona zehatz bati erreferentziarik egiten ez dion informazioak kontrolatu behar den egoera ezagutzeko aukera emango dio kontrolatzeko eginkizuna duenari.

Langileen ordezkariei datu pertsonalak uzten bazaizkie, datuen jakinarazpen horretan adieraziko da sekretua gordetzeko betebeharra dutela datu horiek ezagutzen dituztenek.

ERANSKINA

II.XII.SZ. LANEKO ARRISKUEN PREBENTZIORAKO DATUAK UZTEA

Laneko arriskuen prebentzioari buruzko azaroaren 8ko 31/1995 Legearen 30.3 artikuluak zera dio: «Prebentzio-jarduera gauzatzeko, enpresaburuak ahalbidetu beharko du izendatutako langileek eskura izatea lege honen 18. eta 23. artikuluek aipatu informazioa eta agiriak».

Dokumentazioa aipatzen duen artikulua 23.a da, eta honako hau jasotzen da bertan:

«1.– Enpresaburuak egin eta gorde beharko ditu, aurreko artikuluetan ezarri betebeharren inguruan ondoko agiriak, lan-agintaritzaren esku jartzeko:

a) Lan-arriskuak prebenitzeko plana, lege honen 16. artikuluaren 1. idatz-zatiak ezarritakoa aintzat hartuta.

b) Laneko segurtasun eta osasunerako arriskuen ebaluazioa, lan-baldintzen eta langileen jardueraren aldizkako kontrolen emaitzak barne, lege honen 16. artikuluaren 2.– idatz-zatiko a) paragrafoan xedatutakoaren arabera.

c) Prebentzio-jardueraren plangintza, hartu beharreko babes- eta prebentzio-neurriak barne, eta, hala

ANEXO

II.SC.XII CESIÓN DE DATOS EN LA VIGILANCIA Y PROTECCIÓN DE LAS CONDICIONES DE TRABAJO

La función de vigilancia y protección de las condiciones de trabajo, atribuidas a los distintos órganos de representación de los trabajadores puede llevarse a adecuado desarrollo sin necesidad de proceder a una cesión masiva de los datos referentes al personal que presta sus servicios en la UPV/EHU.

No obstante lo anterior, en el caso de que la vigilancia o control se refieran a un sujeto particular, que haya planteado el problema concreto, será posible la cesión del dato específico de dicha persona.

En los demás supuestos, la función de control quedará plenamente satisfecha mediante la cesión de información de manera agregada o, en su caso, debidamente disociada, es decir, sin poder referenciar los datos a personas identificadas o identificables, que permita a aquélla conocer las circunstancias cuya vigilancia le ha sido encomendada sin referenciar la información en un sujeto concreto.

Si se llegan a ceder datos de carácter personal a representantes de los trabajadores se indicará en dicha comunicación el deber de secreto que obliga a las personas que conozcan dicho dato.

ANEXO

II.SC.XIII CESIÓN DE DATOS EN MATERIA DE PREVENCIÓN DE RIESGOS LABORALES

El artículo 30.3 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales señala lo siguiente: «para la realización de la actividad de prevención, el empresario deberá facilitar a los trabajadores designados el acceso a la información y documentación a que se refieren los artículos 18 y 23 de la presente ley».

El artículo que se refiere a la documentación es el 23 que recoge lo siguiente:

«1.– El empresario deberá elaborar y conservar a disposición de la autoridad laboral la siguiente documentación relativa a las obligaciones establecidas en los artículos anteriores:

a) Plan de prevención de riesgos laborales, conforme a lo previsto en el 16.1 de esta Ley.

b) Evaluación de los riesgos para la seguridad y la salud en el trabajo, incluido el resultado de los controles periódicos de las condiciones de trabajo y de la actividad de los trabajadores, de acuerdo con lo dispuesto en el párrafo a) del artículo 16.2 de esta Ley.

c) Planificación de la actividad preventiva, incluidas las medidas de protección y de prevención a adoptar y,

denean, erabili beharreko babes-tresneria, lege honen 16. artikuluaren 2. idatz-zatiko b) paragrafoan xedatutakoaren arabera.

d) Lege honen 22. artikuluan jaso langileen osasunegoeraren inguruan egindako kontrolak eta kontrol horien emaitzak, aipatu artikuluko 4. idatz-zatiaren azken lerrokadak ezarritakoaren arabera.

e) Langileari lanegun bat baino gehiagoz lan egiteko ezgaitasuna eragin dioten lan-istripuen eta lanbidegaixotasunen zerrenda. Halakoetan, gainera, enpresaburuak egingo du artikulu honen 3. idatz-zatian jaso jakinarazpena.

Transkribaturiko zerrenda horretatik ulertzen da informazio agregatuaren bitartez bete daitezkeela legeak ezarritako helburuak. Alabaina, dokumentazio horrek datu pertsonalak baldin baditu, edo burututako jardueren ondorioz datu pertsonalak ezagutzen badira, lege horretako 37.3 artikuluan jasotzen den lanbide-isilpekoari buruzko betebeharra bete beharko da.

ERANSKINA

II.XIV.SZ. ERREFERENTZIA PERTSONALAK

Arautegi honen testuinguruan, «erreferentzia pertsonalak» terminoak ikasleei edo ikasketak bukatu dituztenei buruzko informazioa eskatu edo emateko ekintza aipatzen du; informazio hori normalean helburutzat lana edo hobekuntza profesionala duen gomendioa izaten da. Erreferentziak emateak askotan datu pertsonalak jakinaraztea eskatzen du.

Datu pertsonalei buruzko legezko arautegira egokitzeko, funtsezkoa da erreferentzia pertsonalen gaineko politika eta praktika berrikustea. Horregatik, UPV/EHUk etorkizunean erreferentzia pertsonalei buruzko politika instituzionala ezarri ahalko du, eta horrela jakin ahal izango da nork eman ditzakeen erreferentziak erakundearen izenean, erreferentzia-eskaerekin nola jokatu behar den, zer informazio-mota eman daitekeen, erreferentzien atzipena nola artikulatzen den, eta abar. UPV/EHUk ziurtatuko du erreferentzia-eskaera jasotzen duen orok ezagutzen dituela gai horien inguruko gomendioak, edo badakiela zein den erreferentzien gaineko politika, halako politikarik zehaztuta egotekotan.

Erreferentziak nola eman.

Etorkizunean norbaiti lana, bekak edo profesionalki aberasteko beste edozein aukera emateko helburua duen pertsona batek eskatzen badu profil zehatz bat duen ikasle edo titulatu baten identitatea, edo UPV/EHUko pertsona jakin bati eskatzen badizkio ikasle edo titulatu zehatz batzuen gaineko ebaluaziori buruzko datuak, honako protokolo hau bete beharko da:

en su caso, material de protección que deba utilizarse, de conformidad con el párrafo b) del artículo 16.2 de esta Ley.

d) Práctica de los controles del estado de salud de los trabajadores previstos en el artículo 22 de esta Ley y conclusiones obtenidas de los mismos en los términos recogidos en el último párrafo del apartado 4 del citado artículo.

e) Relación de accidentes de trabajo y enfermedades profesionales que hayan causado al trabajador una incapacidad laboral superior a un día de trabajo. En estos casos el empresario realizará, además, la notificación a que se refiere el apartado 3 del presente artículo.»

De la relación transcrita se entiende que se pueden cumplir los objetivos de la ley a través de información agregada. No obstante, en el supuesto de que la citada documentación deba contener datos de carácter personal, o que con ocasión de las actuaciones que desarrollen se conozcan determinados datos de carácter personal, se deberá cumplir con el deber de sigilo que le impone el artículo 37.3 de la ley.

ANEXO

II.SC.XIV REFERENCIAS PERSONALES

En el contexto del presente Reglamento, el término «referencias personales» alude a las acciones de solicitar y dar información sobre alumnado o egresados, generalmente a modo de recomendaciones, con fines laborales o de perfeccionamiento profesional. La provisión de referencias implica usualmente la comunicación de datos de carácter personal.

La revisión de la política y la práctica en relación a las referencias personales es una operación básica para la adecuación a la normativa legal en materia de datos de carácter personal. Por ello, la UPV/EHU en el futuro podrá establecer una política institucional sobre referencias personales, en la cual se identifique quién puede facilitar referencias en nombre de la organización, cómo manejar las peticiones de referencias, tipos de información que pueden ser proporcionados, cómo se articula la concesión de acceso a las mismas, etc. La UPV/EHU se asegurará que todas las personas que pudieran recibir una petición de referencias conocen estas recomendaciones y, en su caso, la política sobre referencias elaborada.

Cómo proporcionar referencias.

Cuando una persona, en su calidad de futura empleadora o para conceder becas u otras oportunidades de enriquecimiento profesional, solicita que se le facilite la identidad de alumnado o egresados que cumplen un determinado perfil o, por otro lado, solicita de una determinada persona de la UPV/EHU que proporcione datos evaluativos sobre alumnado o egresados concretos, se ha de cumplir el siguiente protocolo:

1.– Jakinarazi beharko da badaudela erakundeek beren lan-eskaintzak, prestakuntza-planak, plan profesionalak eta abar iragartzeko guneak, eta iragartzen den eskaintza edo aukerari heltzeko interesa dutenek beren burua aurkez dezaketela gaur egun Praktiges eta Lanbila deitzen diren gune horietan.

2.– Erreferentziak UPV/EHUren izenean egiten direla ulertuko da; beraz, erreferentziak egiten dituzten langileek egiten dutenaz jabetu beharko dute, unibertsitateko kideak diren aldetik.

3.– Jakinarazi beharko da unibertsitateko egitura-edo antolakuntza-unitate bakoitzean UPV/EHUren izenean eta unitate horien erabakiz nork eman ditzakeen ikasle edo titulatuei buruzko erreferentziak. Horri dagokionez, printzipio hau aplikatu beharko da: ebalua dezaketenek formalki ebaluatzeko eskumena izan beharko dute; bestalde, ikasle baten nahiz ikasle-talde baten gaitasun orokor eta espezifiko batzuk neurtzeko beste batzuek baino aukera gehiago eta aukera hobeagoak edukitakoak izan beharko dira. Ildo horretatik, ikasle edo titulatuak ebaluatzeko gaituenak izango dira beren tutoreak, praktiketako irakasleak, edo irakaskuntza-ikaskuntzaren prozesuan ikaslearekin hurbileko harreman iraunkorra izan dutenak.

4.– UPV/EHUren izenean hirugarrenei erreferentziak ematen dizkietenek ziurtatu beharko dute erreferentziaren xede den pertsonak nahi duela berari buruzko erreferentzi horiek ematea; hau da, aldez aurretik bere adostasuna lortu beharko dute.

5.– Erreferentziak ematen dituenak horien kopia bat bidali beharko du ikastegiko idazkaritzara edo dagokion egiturara, espediente akademikoarekin batera artxiba dadin.

6.– Erreferentzia guztien oinarrian ikasle edo titulatuek dituzten gaitasunen edo gaitasunak lortzeko dauzkaten bitartekoen ebaluazio edo neurketa egon beharko da. Neurketa hori erabilgarria, bideragarria eta ongi funtsaturikoa izango da; bestalde, pertsonak eta programak ebaluatzeko komunitate zientifikoak eskuarki onartzen dituen estandarrekin bat etorriz egingo da neurketa, estandar horiek hezkuntzaren alorrean aplikatuz.

7.– Erreferentziak egingo dira onartuz datuaren titularrak aukera izango duela berari buruz idatzi dena ikusteko. Gizabanakoak berari buruz idatzi dena ezagutzeko duen eskubideak sendotu egiten du erreferentzia bat egiteko prozesua.

8.– Ez da gomendatzen ahozko erreferentziak ematea; edozein modutan, horrelakorik ematekotan, beharrezkoa izango da aldez aurretik interesdunen adostasuna lortzea. UPV/EHUk ez du hartuko bere langileek ahoz eman ditzaketen erreferentzien gaineko erantzukizunik; izan ere, datu pertsonalen tratamendu horrek duen kalitate faltak arazoak sor ditzake eta ebaluaziorako datuen fidagarritasuna eta balioa galarazi.

1.– Informar que existen espacios (denominados actualmente Praktiges y Lanbila) destinados a que las entidades anuncien sus oportunidades de empleo, planes de formación o profesionales, etc., de tal manera que la totalidad del colectivo potencialmente interesado puede enviar su candidatura a la oferta u oportunidad que se anuncia.

2.– Las referencias se considerarán realizadas en nombre de la UPV/EHU, por lo que la personal que realiza las referencias tendrá que ser consciente de que lo hace como integrante de la Universidad.

3.– Informar de quién puede facilitar referencias sobre alumnado o egresados en nombre de la UPV/EHU en las distintas estructuras y unidades organizativas de la Universidad, a decisión de éstas. Sobre esta cuestión, el principio que ha de aplicarse es que las personas que pueden evaluar a otras son aquéllas que tienen formalmente competencias evaluadoras y que han tenido, en términos comparativos, más y mejores oportunidades para medir algunas competencias generales o específicas de un alumno o alumna o de un grupo de alumnos. En este sentido, las personas más capacitadas para evaluar a alumnado o egresados podrán ser sus tutores, profesorado de prácticas o personas que hayan mantenido una relación cercana y continuada en el tiempo con el alumno o alumna durante el proceso de enseñanza - aprendizaje.

4.– Todas las personas que dan referencias a terceros en nombre de la UPV/EHU deben asegurarse de que la persona objeto de las referencias desea que sean facilitadas, esto es, deberá obtenerse previamente su consentimiento.

5.– La persona que proporcione las referencias deberá remitir una copia de las mismas a la Secretaría del Centro, o estructura que corresponda, para que sea archivado junto al expediente académico.

6.– Toda referencia sobre alumnado o egresados ha de basarse en una medición y evaluación de competencias o recursos de competencias de los mismos que resulte útil, viable y bien fundamentada, de conformidad con los estándares de evaluación de personas y evaluación de programas aceptados comúnmente por la comunidad científica en su aplicación al campo educativo.

7.– Las referencias deben elaborarse con la asunción de que el titular del dato tendrá la oportunidad de ver lo que se ha escrito sobre él. El derecho del individuo a conocer lo que se ha escrito acerca de él incrementa la robustez del proceso de elaboración de una referencia.

8.– No se recomienda la emisión de referencias orales y, en todo caso, para la emisión de las mismas será necesaria la obtención del consentimiento previo de las personas afectadas. La UPV/EHU no será responsable de las referencias orales que puedan ser emitidas por su personal, debido a los problemas derivadas de su falta de calidad en el tratamiento de los datos de carácter personal y la posible pérdida de fiabilidad y validez de los datos evaluativos.

Norberari buruzko erreferentziak nola atzitu.

Interesdunaren adostasunarekin erreferentzia bat ematean, ikaslea ebaluatzen duena ez da derrigorturik egongo ikasle horri erreferentziaren kopia bat ematera. Berari buruz eman diren erreferentziak ezagutu nahi dituen ikasleak ikastegiko idazkaritzan edo dagokion egituran atzitu ahal izango ditu erreferentzia horiek.

Ikasleek espediente akademikoarekin batera artxibaturiko beraiei buruzko erreferentziak ezereztea eskatu ahal izango dute, erreferentzia horiek ezerezteko eskubidea baliatuz.

ERANSKINA

II.XV.SZ. IRAKASKUNTZA-JARDUERAREN EBALUAZIOA

Puntu honi dagokionez, irakaskuntzaren ebaluazioa jasotzen duen UPV/EHUko estatutuetako 160.2 artikulua da garrantzitsuena, eta artikulu horren arabera, irakasleek, sailek, ikastegiek eta ikasleen ordezkariek ebaluazio indibidualen berri izango dute, baita, horrela egin bada, taldeka egindako ebaluazioena ere, irakaslana hobetzera zuzendutako balorazioak egin ditzaten. Kautela guztiak hartuko dira interesdunen eskubideak bermatzeko eta arrazionaltasun, zorroztasun, konfidentzialtasun eta objektibotasun printzipioak errespetatzeko. Interesdunek egokitzat hartuko dituzten alegazioak egiteko aukera ere izango dute.

Edonola ere, irakasleek, sailek, ikastegiek eta ikasleen ordezkariek irakasleen ebaluazioetatik ateratako taldekako emaitzen berri jakin ahal izango dute, ebaluazio horietan interesdunak izatearen baldintza betetzen badute.

Halaber, instantzia horiek irakaskuntzaren ebaluaziotik ateratako emaitza indibidualak eskatu ahal izango dituzte, behar bezala justifikatutako kasuetan; adibidez, ematen duten irakaskuntza hobetzeko xedearekin, sail eta ikastegien ordezkaritzarako kide anitzeko organoek egindako eskariak direnean.

Eskatutako dokumentazioa bidaltzearekin batera gogoraraziko zaie jasotzen duten informazioa ez dela publikoa, eta, beraz, informazio horren edukia isilpean gorde beharko dutela. Sekretua gordetzeko betebeharra betetzen ez duenak diziplinazko erantzukizunak izango ditu.

Cómo dar acceso a una persona a sus propias referencias.

El evaluador o evaluadora de un alumno o alumna, que haya emitido una referencia con el consentimiento de la persona implicada, no está obligado a proveer una copia de la misma a la persona de la que trata la misma. El alumno o alumna que desea conocer las referencias emitidas sobre su persona podrá tener acceso a sus referencias acudiendo a la Secretaría del Centro o estructura que corresponda.

El alumnado tendrá derecho a solicitar la cancelación de las referencias sobre su persona archivadas junto con su expediente académico ejerciendo el derecho de cancelación de las mismas.

ANEXO

II.SC.XV EVALUACIÓN DE LA ACTIVIDAD DOCENTE

Según la normativa universitaria (siendo la más importante al respecto la relativa a la evaluación de la docencia prevista en el artículo 160.2 de los Estatutos de la UPV/EHU), con las cautelas que procedan para garantizar los derechos de los interesados, y con sujeción a los principios de racionalidad, rigor, confidencialidad y objetividad, los resultados de las encuestas relativas a la evaluación de la docencia de carácter individual o, en su caso, agrupados como corresponda, serán comunicados al profesorado, a los Departamentos, a los centros docentes y a los representantes del alumnado a fin de que se realicen las valoraciones oportunas de cara a la mejora de las enseñanzas y sin perjuicio de que se puedan formular las alegaciones que correspondan.

En todo caso, el Profesorado, los Departamentos, los Centros Docentes y los representantes del alumnado podrán acceder a los resultados agregados de las evaluaciones del profesorado en las que se cumpla la condición de interesado.

Asimismo, dichas instancias podrán solicitar resultados de carácter individual de las encuestas relativas a la evaluación de la docencia en supuestos debidamente justificados tales como: solicitudes de los Departamentos y centros docentes realizadas por sus órganos colegiados de representación con el fin de realizar análisis encaminados a la mejora de las enseñanzas que imparten.

Junto con el envío de la documentación que soliciten se les deberá recordar que la información que reciben no es pública y que por tanto, deben guardar sigilo sobre su contenido. En el caso de incumplimiento de tal deber de secreto, responderán disciplinariamente por la falta cometida.

ERANSKINA

II.XVI.SZ. MATRIKULARAKO KLAUSULA-MOTA

Datu pertsonalak babestea: Datu Pertsonalak Babesteari buruzko abenduaren 13ko 15/1999 Lege Organikoaren 5. artikuluari jarraiki, adierazten dizugu zure datuak UPV/EHUren fitxategian sartuko ditugula. Fitxategi horren helburuak zure unibertsitateko ikasketekin du zerikusia.

Datuak atzitu, zuzendu, ezereztu edo datuen aurka egiteko eskubideak balia ditzakezu. Horretarako, idazki bat igorri behar diozu UPV/EHUko DBLO segurtasun-arduradunari helbide honetara:UPV/EHU - Errektoregoa - Sarriena auzoa, z.g. 48940 Leioa (Bizkaia). Idazkiari zure identitatea egiaztatzeko dokumentuaren kopia erantsi behar diozu.

* Nahi izanez gero, unibertsitateko ikastegiek beste klausula batzuk ezarri ahalko dituzte, hirugarrenei datuak uzteko ikasleen adostasuna lortzeko xedez, datuuzte horrek unibertsitatearen helburuekin zerikusirik duenean.

ANEXO

II.SC.XVI CLÁUSULA TIPO PARA MATRÍCULA

Protección de datos: De acuerdo con lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, le informamos que sus datos pasan a formar parte de los ficheros de la UPV/EHU cuya finalidad esté relacionada con sus estudios universitarios.

Puede ejercitar los derechos de acceso, rectificación, cancelación y oposición de sus datos remitiendo un escrito a la persona Responsable de Seguridad LOPD de la UPV/EHU, Rectorado, Barrio Sarriena s/n, 48940 Leioa - Bizkaia, adjuntando copia de documento que acredite su identidad.

* De forma potestativa, los centros universitarios podrán incluir otras cláusulas supervisadas previamente por la persona Responsable de Seguridad LOPD con el objeto de recabar el consentimiento del alumnado para la cesión de sus datos personales a entidades terceras relacionadas con fines universitarios.

EUSKO JAURLARITZA **GOBIERNO VASCO**

LEHENDAKARIORDETZA **VICEPRESIDENCIA**

EHAA EROSTEKO LEKUAK.

Euskal Herriko Agintaritzaren Aldizkariaren aleak Eusko Jaurlaritzaren egoitza hauetan erosi ahal izango dira:

PUNTOS DE VENTA DEL BOPV.

Los ejemplares del Boletín Oficial del País Vasco se pueden adquirir en las sedes del Gobierno Vasco siguientes:

LURRALDE HISTORIKOA TERRITORIO HISTÓRICO	**HERRIA** POBLACIÓN	**EROSTEKO LEKUA** PUNTO DE VENTA	**HELBIDEA ETA TELEFONOA** DIRECCIÓN Y TELÉFONO
Araba Álava	Vitoria-Gasteiz	**Liburudenda. Lakua II eraikina.** Librería. Edificio Lakua II	**Donostia kalea, 1.** c/ Donostia-San Sebastián, 1 945 01 68 66
Bizkaia	Bilbao	**Hiritarrei argibideak eman eta jaramon egiteko Zerbitzua.** Servicio de información y atención al ciudadano.	**Kale Nagusia, 85.** c/ Gran Vía, 85. 94 403 18 08
Gipuzkoa	Donostia-San Sebastián	**Hiritarrei argibideak eman eta jaramon egiteko Zerbitzua.** Servicio de información y atención al ciudadano.	**Andia kalea, 13** c/ Andía, 13. 943 02 33 52