eman ta zabal zazu

Universidad del País Vasco

Euskal Herriko Unibertsitatea

GUÍA DE PROTECCIÓN DE DATOS EN LA GESTIÓN UNIVERSITARIA

www.ehu.eus

GUÍA DE PROTECCIÓN DE DATOS EN LA GESTIÓN UNIVERSITARIA

Universidad del País Vasco / Euskal Herriko Unibertsitatea

Basada en el Reglamento Europeo de Protección de Datos (RGPD) y Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)

Versión adaptada a la Ley 16/2023, de 21 de diciembre, de la Autoridad Vasca de Protección de Datos.

eman ta zabal zazu

Universidad del País Vasco
Euskal Herriko Unibertsitatea

Índice

1. Marco jurídico

La protección de las personas físicas en relación con el tratamiento de sus datos personales es un derecho fundamental, así reconocido en la Carta de los Derechos Fundamentales de la Unión Europea (artículo 8) y el Tratado de Funcionamiento de la Unión Europea (artículo 16).

Este derecho fundamental a la protección de datos garantiza a la persona el control sobre sus datos personales para evitar una utilización ilícita o lesiva de su dignidad y derechos, constituyendo una facultad de autodeterminación de la persona que reconoce su capacidad para disponer y decidir el tratamiento de sus datos por parte de un tercero, sea de naturaleza pública o privada.

Esa protección específica se recoge en el Reglamento (UE) 679/2016 General de Protección de Datos (en adelante, RGPD) que, además, permite a los Estados miembros de la Unión Europea desarrollar contenidos coherentes con esta norma, que se han concretado en la Ley Orgánica 3/2018 de Protección de Datos y Garantía de los Derechos Digitales (en adelante, LOPDGDD) y en la reciente Ley 16/2023, de 21 de diciembre, de la Autoridad Vasca de Protección de Datos.

En este contexto normativo la Universidad del País Vasco/Euskal Herriko Unibertsitatea (en adelante, UPV/EHU) se compromete, dentro del marco de referencia impuesto por la Ley Orgánica 6/2001 de Universidades, a cumplir los derechos y libertades de las personas usuarias en las diversas actividades de tratamiento de datos personales que efectúa, así como en sus relaciones con otras administraciones y entidades públicas u organizaciones privadas, garantizando el cumplimiento de la legalidad vigente y velando porque no se lesionen la privacidad, la reputación o la dignidad de las personas, la transparencia en el uso de la información personal y la no exclusión por motivos de vulnerabilidad.

A este propósito se dirige esta guía que, centrada en el tratamiento de datos personales de la gestión académica y docente, complementa la relativa a la actividad investigadora ya elaborada por la institución, y que tienen por objeto orientar a las personas que gestionan información personal como consecuencia del ejercicio de sus tareas y competencias en la UPV/EHU para contribuir a la comprensión y aplicación de la normativa de protección de datos.

- Esta guía posee un alcance instructivo en la aplicación de la normativa de protección de datos y no genera ningún derecho, obligación o expectativa en tanto esta capacidad pertenece a los textos normativos en la interpretación que de ella efectúan las agencias de protección de datos y los tribunales en razón a la competencia y al ámbito europeo o estatal.
- A tal efecto, ha tenido en cuenta la normativa vigente en materia de protección de datos y su interpretación por parte de la autoridad de control en la materia, así como las orientaciones trasladadas por la CRUE – Conferencia de Rectores de las Universidades Españolas en su Guía sobre la protección de datos personales en el ámbito universitario editada en tiempos de la pandemia y que han sido adaptadas a la UPV/EHU en consideración a sus circunstancias y a su normativa interna.

2. Tratamiento de datos personales en la gestión académica y docente

La docencia o función educativa constituye la misión esencial de las Universidades públicas que se manifiesta en la prestación de un servicio público consistente en proveer de educación superior a la ciudadanía, función encomendada en virtud de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades y restante normativa vinculada.

En su plasmación se desarrolla un conjunto de servicios en que se materializan las enseñanzas universitarias como manifestación de un servicio público comprometido con la transferencia del conocimiento que contribuye al desarrollo y dinamización de la sociedad y que comprende la prestación de servicios dirigidos a la orientación e inserción laboral del alumnado, el desarrollo de actividades vinculadas a la educación superior, tales como la realización de prácticas y estancias en otros centros educativos como parte de la formación universitaria, la realización de acciones formativas para la promoción y fomento de proyectos o la gestión de ayudas y becas.

La ejecución de este conjunto de servicios requiere tratar datos personales para diversas finalidades tales como la admisión de solicitantes, identificación del alumnado, evaluación de conocimientos, control de asistencia a clases y de acceso a instalaciones, acceso y control, así como el uso de recursos electrónicos, evaluación de conocimientos, comunicación de datos a otras instituciones, elaboración de estudios, estadísticas y controles del cumplimiento normativo y, en general, todas aquellas finalidades dirigidas a gestionar el proceso de formación y capacitación del alumnado. Se realizan actividades que no implican el uso de datos personales, como actuaciones de ámbito estadístico o genérico, dirigidas a extraer conclusiones o tomar decisiones, y en las que no se utilizan datos personales.

En el ámbito de la UPV/EHU las finalidades para las que la institución trata datos personales con motivo de la gestión académica y docente se encuentran identificadas en el documento denominado Registro de Actividades de Tratamiento que se encuentra disponible en https://www.ehu.eus/es/web/idazkaritza-nagusia/babestu

Este Registro recoge como finalidades del tratamiento de datos personales, por ejemplo, la gestión de los expedientes académicos del alumnado de la Universidad relativos a de los estudios oficiales junto a todas aquellas actuaciones administrativas y académicas inherentes para la prestación del servicio público de la educación superior en sus distintos ciclos (Grado, Master y Doctorado) bajo cualquier modalidad (presencial, a distancia y on line) y que incluye el proceso de verificación de conocimientos y la expedición de títulos oficiales o el servicio de Biblioteca Universitaria.

Por lo que respecta a la elaboración de trabajos de fin de master (TFM), trabajos de fin de grado (TFG) y tesis doctorales en cuya elaboración concurran datos personales constituyen actividades de tratamiento de datos personales vinculados a la investigación que deben respetar la normativa interna aprobada por la UPV/EHU, particularmente las instrucciones que emita el Comité de Ética de la institución.

En el ejercicio de la función académica y docente la tipología de datos personales que la UPV/EHU requiere se refiere a datos de carácter identificativo tales como identidad y dni, datos de imagen y voz, características personales tales como fecha y lugar de nacimiento, género o nacionalidad, o datos académicos y profesionales, de formación y titulaciones e historial de estudios, e incluso datos de discapacidad de necesaria gestión para la correcta ejecución de la docencia.

Los datos serán conservados por la UPV/EHU, con carácter general, mientras sigan respondiendo a la finalidad para la que fueron obtenidos o en cumplimiento de obligaciones legales.

La legitimación para el tratamiento de estos datos reside en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos atribuidos a la Universidad, interés público que consiste en la prestación del servicio público de educación superior recogido en la Ley Orgánica de Universidades, de modo que la persona titular de los datos personales está obligada a facilitarlos para poder recibir el servicio educativo, no dependiendo, por tanto, de su consentimiento o autorización.

Esta legitimación abarca a las cesiones o comunicaciones de datos por parte de la Universidad, tales como las que se efectúan por ejemplo a bancos y entidades colaboradoras para gestionar el cobro de las tasas académicas que correspondan, o la transmisión de datos a otras universidades a efectos de la gestión de expedientes de traslado, al departamento del Gobierno Vasco y al Ministerio competentes en materia de educación superior, a las agencias de acreditación externas o al servicio vasco de empleo LANBIDE para la realización de encuestas de inserción laboral, así como a entidades que colaboran o participan en la impartición de ciertas enseñanzas, como masters o prácticas.

Sentado lo anterior, a continuación, se expone y analiza el contexto de cumplimiento normativo en la gestión de datos personales en el ámbito de la docencia y la gestión académica para, a continuación, exponer escenarios específicos vinculados a ésta.

El contexto de cumplimiento normativo parte de una consideración básica introducida por el Reglamento Europeo que consiste en el deber de responsabilidad proactiva en el tratamiento de datos personales definido como la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar el cumplimiento normativo en la materia, y que corresponde a la UPV/EHU en tanto responsable del tratamiento.

En aplicación del principio de licitud, transparencia y lealtad los datos pueden ser tratados solo si existe una habilitación para ello. A esa habilitación la norma lo denomina base o título jurídico, de modo que cuando se pretenda tratar datos personales deberá analizarse si dicha base o título existe y es aplicable al caso concreto. Su determinación no es caprichosa, sino que ha de ser la que se ajuste y acomode a alguna o algunas de las bases o títulos contemplados por el Reglamento General Europeo de Protección de Datos y contemplados en el artículo 6 (para datos básicos u ordinarios) y en el artículo 9 (para categorías especiales de datos).

De todos los permisos o habilitaciones contempladas en dichos artículos, los títulos aplicables más adecuados en el ámbito de la docencia y gestión académica de una Universidad pública serán tanto el interés público o el ejercicio de competencias públicas, como el cumplimiento de obligaciones legales, archivo e interés público, que se regulan en los artículos 6.1.b) y 6.1.c) RGPD. Por tanto, sólo se acudirá a otras bases o títulos habilitantes del tratamiento, como pudiera ser el consentimiento de la persona o el interés legítimo de la Universidad, cuando el tratamiento de datos no pueda considerarse que integra la misión realizada en interés público que corresponde a una Universidad pública y que es proveer de educación superior a la ciudadanía que tiene encomendada en virtud de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades y restante normativa vinculada.

Así, es preciso distinguir entre la actuación como servicio e interés público que realiza la UPV/EHU en la prestación de educación superior, de otras como, por ejemplo, el servicio editorial o el envío de información comercial en alguna actividad que se considere un servicio remunerado, por cuanto, tratándose de una actuación de carácter mercantil de la institución, debe basarse o bien en el interés legítimo de la Universidad de realizar este tipo de actuación divulgativa o comercial, actividad que encajaría en la previsión del artículo 6.1.f) RGPD o bien en el consentimiento de la persona contemplado en el artículo 6.1.a) RGPD.

Otro ejemplo de distinción de bases habilitantes del tratamiento lo constituye el tratamiento de los datos personales del colectivo de personal empleado. El tratamiento de datos personales que requiere la gestión de su actividad laboral, desde su contratación, gestión de la relación laboral, hasta la finalización de su vínculo con la institución, y que comprende actividades de tratamiento de datos necesarios por ejemplo para la elaboración de nóminas y seguros sociales, licencias, formación, ascensos o concursos, prevención de riesgos laborales, relación con la representación del personal, gestión de dietas y viajes, entre otras muchas, se basa en la relación o vinculo jurídico entre la persona empleada y la Universidad, contemplado en el artículo 6.1.b) RGPD, y no se basa ni en el interés público ni en el consentimiento de la persona.

En todo caso, los datos objeto de tratamiento deben ser los estrictamente necesarios y adecuados a los fines para los que son tratados, lo que requiere realizar un juicio o valoración de proporcionalidad en cuanto a calidad, idoneidad y necesidad de tratar dichos datos en el contexto universitario.

Asimismo, la conservación de esos datos debe limitarse en el tiempo al logro de los fines que el tratamiento persigue. Para ello deben tener en cuenta los motivos o finalidad para la que se necesitan los datos, así como las obligaciones legales de conservarlos durante un tiempo determinado conforme a la legislación universitaria. Por ejemplo, los resultados académicos se conservarán indefinidamente ya que es responsabilidad de la institución certificar el expediente académico. En todo caso, la limitación del período de conservación no implica que los datos personales deban eliminarse, sino que una vez que ya no son necesarios permanezcan bloqueados durante un tiempo que será el necesario para atender posibles reclamaciones, requerimientos o cumplimiento de obligaciones por ejemplo de tipo tributario, judicial o de inspección en el período de tiempo en que dichas acciones puedan ejercerse conforme a la legislación que resulte de aplicación.

Naturalmente, toda actuación en protección de datos está presidida por el deber de confidencialidad de las personas que tratan o gestionan esos datos, que se mantiene aún y cuando éstas dejen de tener vínculo profesional con la institución, y por el deber de seguridad dirigido a garantizar que se adopten medidas organizativas y técnicas que garanticen una protección contra el tratamiento de datos no autorizado o ilícito y contra su pérdida, destrucción o daño accidental.

Titularidad y tratamiento

La normativa de protección de datos se centra en la persona física, en tanto a ella pertenece la titularidad de su información personal y que se identifica con la persona física viva cuya identidad se puede determinar, directa o indirectamente, a través de un conjunto de información. Los datos personales son siempre titularidad de la persona y no de las organizaciones que los tratan en tanto se limitan a gestionar dicha información en ejercicio de las tareas o atribuciones que les competen.

En este contexto, la UPV/EHU será considerada responsable de los tratamientos de datos que efectúa y que se encuentran contenidos en su Registro de Actividades de Tratamiento (RAT) que, como se ha indicado precedentemente, se puede consultar en disponible en https://www.ehu.eus/es/web/idazkaritza-nagusia/babestu

Puede darse la circunstancia de que la UPV/EHU colabore con otras organizaciones en una actuación conjunta que requiere que todas ellas conozcan, compartan y traten datos personales. En tal caso, cada una de dichas organizaciones será corresponsable del tratamiento en la parte de gestión que le competa a cuyos efectos se deberá formaliza entre las entidades corresponsables un acuerdo o convenio que determine

las funciones o tareas que corresponden a cada una y las consecuentes obligaciones por lo que respecta al tratamiento de datos personales. Es el caso de un convenio de colaboración entre dos Universidades para el intercambio de estudiantes que, firmado por ambas instituciones, deberá reflejar e identificar con claridad las actividades de tratamiento que cada institución efectúa en el marco de dicha colaboración, con expresión concreta de las actividades de recogida, conservación, alojamiento, cesiones a terceros o utilización secundaria de la información, asumiendo cada parte su responsabilidad respecto de la adecuada gestión de datos personales requerida por el ejercicio de las tareas que le competen con motivo del acuerdo suscrito.

Es necesario distinguir la figura de la UPV/EHU como responsable del tratamiento de datos personales de la figura del ***Delegado de Protección de Datos (DPD o DPO)*** cuya función es la de apoyo a la institución como responsable en esta materia, y que puede desempeñar sus funciones de manera interna o externa pero en todo caso independiente, esto es, sin presiones o indicaciones de la institución.

Finalmente, también es preciso diferenciar estas figuras de la de Encargado del Tratamiento que se refiere al proveedor de servicios contratado por la institución Responsable del Tratamiento y para cuya ejecución requiere el acceso y gestión de datos personales de personas físicas.

Fijado el contexto general a continuación se abordan en los sucesivos epígrafes escenarios específicos que requieren de una mayor precisión u orientación en lo que respecta al cumplimiento normativo en materia de protección de datos en el ámbito de la gestión académica y docente por ser ámbitos donde concurre una mayor controversia en gran medida derivada de nuevas modalidades de formación a distancia y utilización de medios telemáticos.

3. Docencia en el entorno online

Se tratará a continuación la problemática de la gestión de datos personales en relación con la docencia online, con algunos ejemplos o áreas especialmente problemáticas, o que han sido tratadas de forma específica por las Agencias de protección de datos.

Uso de herramientas de docencia virtual

Las herramientas de docencia virtual realizan un tratamiento de datos personales y, por tanto, deben cumplir con todos los requisitos de la normativa aplicable. A tal efecto, deben utilizarse las herramientas indicadas por la UPV/EHU en tanto éstas disponen de las valoraciones necesarias en términos de cumplimiento legal y de seguridad adecuadas entre las que se encuentra la elección de proveedoras con garantías suficientes de cumplimiento legal. Cualquier actuación al margen de esta previsión puede generar un riesgo excesivo o el incumplimiento de alguna previsión legal tanto en materia de tratamiento o de seguridad de los datos personales.

Grabación de las clases docentes

Circunstancias tales como la declaración del estado de alarma por motivo de la pandemia imposibilitaron la celebración de clases presenciales lo que generalizó la realización de clases virtuales o por videoconferencia. En todo caso, y con independencia de la circunstancia motivadora de la realización de la actividad docente en modo no presencial, la emisión y grabación de una clase debe ser valorada en relación con las siguientes funciones:

- Opción de que se ofrezca la posibilidad de su visionado posterior en modelos de teleformación asíncrona; esto es, en un formato en que la interacción entre docente y estudiantes se realiza en espacio y momentos distintos. Debe valorarse el periodo de permanencia y el nivel de acceso a a la formación, restringiendo ambos.
- Garantizar la accesibilidad a los contenidos por parte de estudiantes que, por circunstancias tecnológicas, personales o de salud, entre otras, no se hayan podido conectar a la emisión síncrona.
- Constituir un material de estudio para la preparación de la evaluación, que tenga un periodo de permanencia vinculado y coordinado con el periodo de evaluación.

Las grabaciones de imagen, sonido y texto, además de constituir tratamiento de datos personales, pueden afectar a contenidos protegidos por la propiedad intelectual, tanto por los contenidos manifestados, conocimientos expuestos o por los materiales utilizados. Desde la perspectiva de la protección de datos y en aplicación del principio de finalidad, las grabaciones únicamente deben ser utilizadas en el entorno de la asignatura, y tanto el profesorado como el alumnado debe ser informados sobre el tratamiento de

datos que se realiza, de su permanencia y de los derechos que les asisten, incluso la posibilidad de acudir a la Autoridad Vasca de Protección de Datos.

Las grabaciones de la docencia realizadas por el profesorado se alojarán en las plataformas de la Universidad y podrán estar disponibles en formato asíncrono mientras sigan respondiendo a los fines para las que se realizaron dichas evaluaciones, es decir para poder ser revisadas o visionadas por el alumnado que se encuentra matriculado en dicha asignatura, y siempre vinculado su permanencia a la docencia.

En este sentido únicamente el alumnado de la asignatura o grupo de que se trate debería poder acceder a las grabaciones que están alojadas en las herramientas de la Universidad. En cualquier caso, se procurará que en las sesiones de docencia no se graben, traten ni conserven datos de carácter personal de cualquier tipo que permitan identificar a personas pertenecientes a colectivos vulnerables como personas con discapacidad, víctimas de violencia de género o acoso y, en general, pertenecientes a colectivos vulnerables. Esto exigirá cierta revisión por parte de las personas responsables de contenidos y gestión.

Con carácter general, se recomienda emplear la grabación utilizando el sistema de aula virtual por defecto. Así, y a fin de respetar al máximo los derechos del alumnado, se deberá:

- Optar preferentemente por las interacciones en el chat, frente a las interacciones verbales.
- Favorecer las preguntas e interacciones sin activar la cámara, si no se considera necesario.
- Además, se deberá advertir al alumnado de que no podrá realizar grabaciones de las sesiones docentes, siendo responsable en caso contrario de dicha actuación.

Información relativa a la grabación de las clases

Las intervenciones en clase se consideran una parte más de la actividad docente, tanto en las clases presenciales como no presenciales Por lo tanto, es conveniente advertir que las grabaciones no podrán ser usadas para otros fines, ni descargadas y en todo caso informar que la clase va a ser grabada incluyendo esta información bien en el punto general de acceso al aula virtual, al inicio de cada asignatura, antes del comienzo de cada sesión o a través de un mensaje remitido a la comunidad universitaria, recomendándose que al inicio de la clase, antes de comenzar la grabación se advierta al alumnado que la sesión (imagen, sonido y/o chat) va a ser grabada de modo que puedan desactivar su cámara/micrófono y en su caso participar a través del chat.

Cualquiera de estas opciones se considera adecuada, al respetar la normativa de protección de datos.

En particular debe advertirse al alumnado que debe preservar su espacio de interacción, de manera que se proteja la intimidad familiar y la de terceras personas que pudieran aparecer y ser captadas por la grabación para evitar que esta captación de imágenes se produzca y afecte a derechos de terceras personas.

Difusión y publicación de las clases grabadas

Únicamente se deben utilizar los sistemas corporativos de la UPV/EHU, como se ha indicado. La descarga, difusión, distribución o divulgación de la grabación de las clases y particularmente compartir y difundir en redes sociales o servicios dirigidos a compartir apuntes puede atentar contra el derecho fundamental a la protección de datos, el derecho a la propia imagen y los derechos de propiedad intelectual. Tales usos se consideran usos prohibidos y podrían generar responsabilidad disciplinaria, administrativa o civil de la persona infractora.

Las grabaciones sólo podrán ser accesibles en el aula virtual oficial de la Universidad. Las grabaciones fuera de los entornos oficiales no deben realizarse en ningún caso dados los riesgos que conllevan.

Período de conservación de las clases grabadas online

Con carácter general las grabaciones estarán disponibles como máximo durante el correspondiente curso académico o periodo lectivo, mientras sigan respondiendo a los fines para las que se realizaron; esto es, para poder ser revisadas o visionadas por el alumnado que se encuentra matriculado en dicha asignatura y salvo que formen parte de las evidencias para la evaluación del alumnado. Ello sin perjuicio de que la Universidad podrá conservar una copia debidamente bloqueada para el cumplimiento de obligaciones legales que correspondan a la institución. En el caso de que el o la docente quisiera reutilizar estos materiales para otras actividades académicas deberá eliminar previamente cualquier dato personal de estudiantes o terceras personas.

Utilización de dispositivos propios del alumnado para el seguimiento de la docencia online.

En el caso de que para el seguimiento de las clases se empleen dispositivos compartidos se recomienda crear perfiles que preserven la privacidad de cada persona que vaya a utilizarlos.

Asimismo, debe indicarse al alumnado que se instale en sus ordenadores a los efectos de la docencia solo aplicaciones para las que la Universidad disponga de licencia y se hayan recomendado, en tanto analizadas por la institución como respetuosas con la privacidad y la seguridad.

4. Tratamientos de datos personales en la evaluación de conocimientos del alumnado

Grabación de imágenes y sonido del alumnado durante la realización de pruebas de evaluación orales síncronas

A continuación, se distingue la realización de pruebas orales síncronas (pruebas orales en tiempo real y a distancia), de las pruebas escritas síncronas (pruebas escritas en tiempo real y a distancia), disponiendo la UPV/EHU de normativa específica adoptada respecto a la forma de su realización.

En relación con las pruebas orales síncronas la finalidad de la grabación únicamente podrá ser la de garantizar el proceso de verificación de conocimientos del alumnado, realizándose un seguimiento de la prueba oral por el profesorado a través de los sistemas de videoconferencia, monitorizando la realización de las pruebas de evaluación a distancia.

El desarrollo de las pruebas de carácter oral podrá recogerse o grabarse en formato sonido, al constituir un derecho del alumnado, tal y como establece la normativa reguladora de la evaluación del alumnado en las titulaciones oficiales de grado. Y ello con la finalidad de comprobación o revisión de la evaluación.

Dadas las funcionalidades que ofrece el sistema establecido institucionalmente el profesorado podrá realizar una grabación en formato de video y/o audio de la prueba utilizando las herramientas corporativas prevista por la Universidad eGela y BBC, siempre con finalidades docentes o de comprobación de pruebas de evaluación.

Las grabaciones realizadas de una prueba de evaluación a distancia deberán ser conservadas por el departamento como mínimo hasta la finalización del curso siguiente salvo que haya un recurso pendiente en cuyo caso deberán mantenerse hasta la su resolución. De esas grabaciones no podrán ser empleadas para fines diferentes a la exclusiva verificación de los aprendizajes del alumnado, revisión de calificaciones y recursos ulteriores, en su caso.

Al inicio de la prueba el profesorado deberá informar al alumnado de la conveniencia de ejercer el derecho a la grabación de la prueba oral ya que puede ser de utilidad para la revisión de las calificaciones. Durante la realización de la prueba el alumnado permitirá en el equipo informático el uso del dispositivo de transmisión de imagen y sonido correspondiente siguiendo las indicaciones del profesorado ante quien se desarrolle la prueba.

Cualquier estudiante podrá ser requerido o requerida a identificarse previamente y durante el desarrollo de la prueba correspondiendo al profesorado recoger las evidencias del desarrollo de la prueba que junto a la grabación del sonido y en su caso imagen sean necesarias para el correcto ejercicio de la función evaluadora con plenas garantías de equidad y justicia para el alumnado.

Grabación de imágenes y sonido del alumnado durante la realización de pruebas de evaluación escritas síncronas

El profesorado podrá seguir la realización de la prueba individualmente a cada alumna o alumno o en grupo a través de los sistemas de transmisión de imagen y sonido. Durante la realización de la prueba escrita el alumnado activará el dispositivo de transmisión de imagen en aquellos momentos en los que sea requerido por el profesor o profesora teniendo en cuenta que el alumnado realiza la prueba en espacios de su propio domicilio, y siempre a los efectos de verificación de identidad o de corrección en la realización de la prueba.

Por lo que respecta a la transmisión de sonido durante la realización de estas pruebas el dispositivo de transmisión de sonido o micrófono deberá activarse desde el principio de la prueba y permanecerá en ese estado hasta que finalice la misma a menos que se indique otra cosa por parte del profesorado ante quien se desarrolla la prueba.

Durante el desarrollo de la prueba escrita no se realizarán grabaciones de imagen ni de sonido.

Cualquier estudiante podrá ser requerida o requerido a identificarse previamente y durante el desarrollo de la prueba.

Corresponde al profesorado recoger todas las evidencias del desarrollo de la prueba que sean necesarias para el correcto ejercicio de la función evaluadora con plenas garantías de equidad y justicia para el alumnado.

Elaboración de videotutoriales por el alumnado y posterior publicación

La elaboración y ulterior publicación o difusión de los videotutoriales se ha de fundamentar en el previo consentimiento otorgado por estudiantes o personas que aparezcan en los videos, salvo que se trate de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público.

Negativa del profesorado a ser grabado durante el desarrollo de una prueba de evaluación y consecuencias

La base de legitimación para el tratamiento de datos personales del personal de la Universidad ya sea personal funcionario o laboral no se basa en el consentimiento, sino que se sustenta en la relación jurídica establecida sobre la base de su nombramiento público en el caso de los cargos públicos, o de su contratación. De ese modo, en el caso de la grabación de una prueba de evaluación, el tratamiento de sus datos obedece al uso instrumental de su figura en el ejercicio de los derechos del alumnado a ser evaluado con objetividad y por seguridad jurídica del proceso.

Solicitud de acceso de estudiantes a sus imágenes o petición de que se rectifiquen o cancelen

Como parte de las facultades que integran el derecho a la protección de datos personales, en relación con aquellos casos en los que la grabación sirva como evidencia de la evaluación, el alumnado podrá solicitar el acceso a sus imágenes objeto de grabación, bien como evidencia de su prueba de evaluación, para lo que deberá seguir el correspondiente trámite de revisión previsto en la normativa académica; bien como facultad que le otorga su derecho de protección de datos, para lo cual habrá que tener en cuenta el periodo de conservación de dichas imágenes. El periodo de conservación estará directamente relacionado con la finalidad de la grabación, como se ha indicado.

En relación con la posibilidad del alumnado de solicitar la rectificación de sus imágenes en las pruebas de evaluación, y por su propia naturaleza, no será posible realizar rectificaciones si las imágenes están dirigidas a dar fe de la realización de la prueba de valoración.

En el mismo sentido, en relación a la solicitud de supresión de datos personales, que será denegada prevaleciendo el deber de conservación en aplicación de la normativa académica correspondiente.

Cualquier reclamación denegada puede ser remitida por el alumnado a la Autoridad Vasca de Protección de Datos.

Conservación de las pruebas de evaluación grabadas online

La conservación de las pruebas de evaluación, ya sean realizadas de forma presencial o de forma online, deberá atenerse a las normas de conservación establecidas por la UPV/EHU, que podrán ser eventualmente revisadas por la Autoridad Vasca de Protección de Datos.

El Estatuto del Estudiante Universitario indica que será el profesorado responsable de la asignatura evaluada el que deberá conservar las pruebas y sus evidencias hasta la finalización del curso académico siguiente en los términos previstos en la normativa universitaria general y de la propia Universidad. En los supuestos de petición de revisión o de recurso contra la calificación y, de acuerdo con la citada normativa, deberán conservarse hasta que exista resolución firme.

La conservación de las pruebas de evaluación y sus evidencias no debe realizarse en equipos personales propios sino a través de los espacios virtuales habilitados por las Universidades como, por ejemplo, las aulas virtuales. Asimismo, en caso de no resultar posible la portabilidad de la información del proceso de evaluación se deberá disponer de un acuerdo de servicio con el proveedor de la herramienta que garantice la durabilidad y accesibilidad a las evidencias.

5. Acceso y publicación de datos personales del alumnado

Acceso a datos del alumnado por progenitores

La facultad de acceso a la información académica integra el conjunto de deberes y derechos que corresponden a padres y madres o personas tutoras legales dentro de su obligación de educar y que ampara la cesión de los datos académicos, salvo que en virtud de resolución judicial se excluya el ejercicio de la patria potestad o concurran circunstancias excepcionales en un caso concreto.

Por otra parte, la circunstancia de dependencia económica, que debe examinarse en cada caso, está vinculada a que se abone una pensión de alimentos o se financien los gastos de subsistencia del alumno o alumna de modo tal que el interés legítimo lo ostentará la persona de quien sea económicamente dependiente.

Asimismo, en un escenario de modificación de la pensión de alimentos, la Agencia Española de Protección de Datos considera que la comunicación de los datos está permitida en base al interés legítimo de la persona progenitora conforme al derecho que le otorga la legislación civil, en concreto el artículo 152 del Código Civil, toda vez que tal información debe aportarse como prueba en un procedimiento judicial y tal derecho parece prevalecer sobre los intereses y derechos del alumno o alumna, sin que ello obste a que pueda ejercer su derecho de oposición a tal tratamiento. Por ejemplo, no existiría esa presunción de interés legítimo si el o la estudiante mayor de edad acredita que es independiente económicamente y ha decidido voluntariamente no mantener relaciones con sus progenitores.

Por consiguiente, deberá examinarse, caso a caso:

1. El concreto interés legítimo que ostenta quien solicita los datos.
2. Si el conocimiento de los datos que constan en la Universidad es necesario para la finalidad perseguida por la persona solicitante.
3. Si el interés legítimo ostentado ha de prevalecer sobre los derechos y libertades del alumno o alumna a quien debe informarse a fin de que pueda ejercer, si así lo considera, su derecho de oposición al tratamiento.

Contacto solicitado por el profesorado

La solicitud por parte del profesorado de acceso a los datos de contacto de un o una estudiante que no pertenece al grupo de su clase (tales como correo electrónico o teléfono) requiere del previo consentimiento de la persona, salvo que, en casos puntuales, por una finalidad docente pueda ser necesario en el marco de la actividad académica tengan acceso a esta información.

Contacto para reunión de promociones

El acceso a los datos de contacto para organización de reuniones para celebrar el aniversario de personas egresadas de una promoción requerirá del previo consentimiento de éstas. La Autoridad Vasca de Protección de Datos ha establecido doctrina en cuanto al uso secundario de los datos para finalidades de este tipo, obteniendo datos de personas empadronadas de un ayuntamiento para una actividad puramente privada, o cuando menos, al margen de la actividad competencia de la Administración ordinaria.

Publicación de las calificaciones

La publicación de las calificaciones en un proceso de evaluación online sigue las mismas reglas que su publicación durante un proceso de evaluación presencial debiendo ser publicadas en los espacios virtuales habilitados a tal fin y a los que sólo pueda acceder el o la alumna, nunca en espacios abiertos a los buscadores ni en un tablón de anuncios.

Por otro lado, atendiendo al principio de finalidad del tratamiento, la publicación de las calificaciones en las aulas virtuales se mantendrá accesible durante el periodo previsto en la normativa académica, garantizando su conocimiento por las y los interesados, así como el ejercicio de los derechos de revisión y, en su caso, reclamación.

Publicación en blog privado de un profesor o profesora de las calificaciones de estudiantes

Se trata de un canal de comunicación al margen de la función docente universitaria, salvo que la normativa interna de la Universidad lo califique como herramienta profesional al servicio de la institución. Por lo tanto, de su contenido será responsable el profesor o profesora, que deberá observar la normativa de protección de datos en tanto incluye información de carácter personal.

En todo caso, no se publicarán en dicho blog las calificaciones de sus estudiantes por cuanto entra en juego que la persona lo consienta sino la proporcionalidad y finalidad de difundir estos datos siendo así que el medio para ello es el dispuesto oficialmente por la Universidad a través del aula virtual.

Por lo tanto, ni siquiera el consentimiento puede hacer que sea legítima esta publicidad.

Acceso a datos de becas y ayudas al estudio concedidas

La publicación del listado de personas beneficiarias (nombre y apellidos), con indicación del importe de la beca concedida a estudiantes tiene suficiente habilitación en normas con rango legal -normativa de subvenciones y ayudas económicas- por lo que no se requiere el consentimiento de aquéllas, al prevalecer el interés público en su conocimiento, siempre atendiendo al principio de minimización que apunta a publicar los datos personales absolutamente imprescindibles por necesarios y a la forma limitada de publicar

datos personales que prevé la Disposición Adicional Séptima de la LOPDGDD en la orientación interpretativa que de ella ha efectuado la Agencia Española de Protección de Datos.

En todo caso, y para satisfacer el derecho de acceso a la información pública será suficiente con indicar el enlace del correspondiente portal de transparencia donde aparece publicada esa información objeto de publicidad activa.

No obstante, hay que tener en cuenta que determinadas ayudas socioeconómicas pueden tener como objeto la atención a personas en situación de vulnerabilidad social, por lo que, debe preservarse la identidad de las personas beneficiarias, aplicando para ello lo dispuesto en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, (LPACAP).

Asimismo, será posible la comunicación a instituciones públicas o privadas que tengan suscritos acuerdos de colaboración con la UPV/EHU para la concesión de becas al alumnado, limitando dicha comunicación a los datos estrictamente necesarios, y sin perjuicio del deber de informar de esta circunstancia a las personas solicitantes en las bases de cada convocatoria.

Datos académicos de cargos públicos

La relevancia pública de una persona es un criterio que, salvo que se acredite unas circunstancias excepcionales concretas, hace que prevalezca el interés público en el acceso a la información curricular, considerando que al representante público debe exigírsele, como parte sustancial de su proyección y relevancia institucional, la máxima transparencia de su perfil académico y profesional.

En el ámbito universitario es razonable circunscribir el concepto de cargo público, a falta de una regulación expresa, a las personas titulares de los órganos de gobierno y representación de las universidades públicas previstas en la Ley Orgánica 6/2001, de Universidades.

Por ello, cuando se solicite el acceso a datos académicos de un cargo público, en principio habría prevalencia del interés general en el conocimiento de la preparación académica de quienes asumen los más altos puestos en la estructura administrativa; esto es, al interés legítimo contemplado en el artículo 6.1.f) RGPD.

6. Comunicación o cesión de datos personales

Comunicación o cesión de datos académicos entre unidades de la misma Universidad o hacia otras instituciones públicas

El tratamiento de datos entre áreas o unidades dentro de la Universidad no tiene la consideración jurídica de comunicación o cesión si la comunicación es necesaria para la gestión administrativa de que se trate y quede el acceso limitado a aquellas personas por razón del cumplimiento de sus tareas.

Específicamente, debe hacerse pública, como mínimo, las resoluciones de autorización o reconocimiento de compatibilidad que afecten a personal empleado público, así como las que autoricen el ejercicio de actividad privada y cese de los altos cargos según la normativa que resulte de aplicación.

Otra interpretación habría de hacerse cuando se trate de entidades del entorno de la Universidad, pero con personalidad jurídica propia, como institutos de investigación, fundaciones o spin off creadas para distintos fines.

Comunicación de datos personales de estudiantes para la realización de prácticas a una empresa o institución

La cesión será posible en cumplimiento del correspondiente acuerdo de colaboración basado en el interés público o en la relación jurídica que se establece entre alumnado, empresa o institución y Universidad.

Tanto empresas o instituciones colaboradoras con la Universidad serán corresponsables del tratamiento de los datos personales, de modo que cada parte será responsable del tratamiento de los datos del alumnado en función de la tarea o competencia que asume en función del convenio o acuerdo.

Comunicación a centros externos de certificados relativos a la no comisión de delitos sexuales para la realización de prácticas que impliquen contacto habitual con menores

Este tratamiento de datos consistente en recabar los certificados negativos de comisión de delitos sexuales de estudiantes de la Universidad que, en el desempeño de sus prácticas en centros educativos, tengan relación profesional con personas menores de edad, se fundamenta en la Ley 26/2015, de modificación del sistema de protección a la infancia y a la adolescencia, que recoge como obligatorio que quienes trabajen con menores de forma habitual presenten un certificado negativo de antecedentes penales relativos a delitos sexuales. Por tanto, el fundamento o permiso habilitante de esta comunicación es el cumplimiento de una obligación legal.

Cesión de datos personales de estudiantes a la policía

La comunicación será lícita siempre y cuando se cumplan las siguientes condiciones: (1) acreditar 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 y que, tratándose de datos especialmente protegidos, sean absolutamente necesarios para los fines de una investigación concreta, (2) que se trate de una petición concreta y específica, y en ningún caso solicitudes masivas de datos (3) que la petición se efectúe con la debida motivación, y (4) que los datos sean cancelados cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

Esta comunicación de datos se efectúa en base al cumplimiento de obligaciones legales ya que existe un deber de colaboración con los Juzgados y Tribunales y con el Ministerio Fiscal conforme a lo dispuesto en la Ley Orgánica 6/1985, del Poder Judicial y el Estatuto Orgánico del Ministerio Fiscal. Y también de acuerdo con lo previsto en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

A tal efecto, constituye una buena práctica no atender peticiones de documentación solicitadas verbalmente y aquéllas que sean genéricas, sin perjuicio de requerir la correspondiente subsanación.

7. Uso de medios tecnológicos

Aplicaciones para dispositivos móviles

El acceso a los datos personales de estudiantes, tales como datos académicos o de contacto, por parte de la organización que da soporte a las aplicaciones móviles de la Universidad no requiere el consentimiento de la persona en tanto este acceso se produce como consecuencia de la prestación del servicio a la institución. Esta circunstancia otorga a la proveedora la condición de encargada de tratamiento de la Universidad debiendo ajustarse a las condiciones que deben quedar plasmadas en el contrato o clausulado de encargo de tratamiento que debe formalizarse entre la institución y la proveedora del servicio y que recoge las obligaciones que asume respecto de la gestión de datos personales conforme a las exigencias impuestas por el Reglamento Europeo de Protección de Datos.

Este amparo en la prestación del servicio para la Universidad o se extiende a las utilidades comerciales de la aplicación que vaya a realizar la proveedora del servicio para lo cual será necesario el previo consentimiento del o de la estudiante al no entrar este supuesto en las finalidades propias de la institución universitaria y para las que contrató el servicio.

Creación de grupos entre profesorado y alumnado con aplicaciones de mensajería instantánea

Se requiere el consentimiento de cada una de las personas que vayan a participar en el grupo, al no entrar este supuesto en las restantes bases jurídicas de legitimación del tratamiento contempladas en el RGPD. A tal efecto, es recomendable reconducir el uso de plataformas a los medios técnicos establecidos por la Universidad como es el caso de plataformas institucionales de apoyo a la docencia o listas de distribución.

Solicitud de baja de las listas de distribución de la Universidad

Una lista de distribución es un conjunto de direcciones de correo electrónico corporativo asociadas a una única dirección de correo para enviar ciertos mensajes o anuncios con un contenido de interés general a grupos de personas integrantes de la lista de manera ordenada. Además, constituye una herramienta muy útil para grupos de trabajo, debates o temas, cuyos miembros deban estar permanentemente informados.

En ningún caso se podrán utilizar las listas de distribución corporativas para la distribución de información ajena a las finalidades de la UPV/EHU.

Toda lista de distribución tendrá un nombre de lista y una dirección de correo electrónico. Asimismo, cualquier lista de distribución debe tener una persona administradora, quien se responsabilizará de crear la lista y de gestionarla adecuadamente con arreglo a las directrices marcadas por la Gerencia. En su caso, la lista también podrá tener una persona moderadora, cuya función consistirá en aprobar o denegar la distribución de mensajes dirigidos a lista y en aprobar o denegar las peticiones de suscripción. Sin perjuicio de lo cual la función moderadora la podrá asumir la persona administradora de la lista de distribución. Tanto una como otra figura deberán ser personal de la UPV/EHU en activo.

Sólo excepcionalmente, se podrán suscribir direcciones de correo electrónico no corporativo.

Al objeto de no incurrir en prácticas abusivas y en usos incorrectos del correo electrónico, la difusión masiva de información de interés general, electoral, sindical o laboral deberá efectuarse a través de estas listas de distribución, procurando, en la medida de lo posible, evitar el uso de adjuntos y utilizando enlaces a los puntos en los que pueda publicarse dicha información. El régimen de autorización, funcionamiento y condiciones de uso de las listas de distribución de la Universidad serán establecidos por la Gerencia.

Además, y para la difusión de la información de carácter sindical o laboral, la UPV/EHU creará listas de distribución asociadas a una dirección de correo electrónico por cada sección sindical del ámbito de la UPV/EHU, recayendo sobre la institución universitaria la asunción de las obligaciones derivadas de la legislación sobre protección de datos de carácter personal y de las derivadas de la gestión de dichas listas, bajo la competencia de la Autoridad Vasca de Protección de Datos..

8. Tratamiento de datos personales relativos a material audiovisual y videovigilancia

Uso de imágenes realizadas en actividades académicas y su posterior difusión en el canal de noticias de la página web de la Universidad o en las redes sociales institucionales

La circunstancia de que la realización de las fotos o la grabación de los videos se produzcan durante un acto público no excluye el consentimiento de las personas grabadas o fotografiadas, salvo que:

1. Se trate exclusivamente de captar la imagen de las personas asistentes de forma accesoria y sin posterior divulgación, o
2. Se tomen en un acto de interés histórico, científico o cultural relevante.

A este respecto es necesario distinguir a personas que ejercen un cargo público o una profesión de notoriedad o proyección pública, puesto que se estaría ante un interés público con amparo en la LO 1/1982 de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

En los restantes supuestos se requiere el consentimiento de las personas para ser captada su imagen y para su posterior difusión. En el caso de personas menores de catorce años, dicho consentimiento deberá ser otorgado por el titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

En el caso de divulgación o utilización de imágenes de personas miembros o ex miembros de la comunidad universitaria o de terceras personas en acciones promocionales de la Universidad, en memorias, guías, revistas, proyectos de innovación docente con fines de difusión de la metodología en entornos académicos o científicos externos, entre otros, se requiere el previo consentimiento de la persona, salvo en el caso de que se trate de un cargo público de la Universidad en tanto concurre un interés público relativo a su participación en tal condición.

En definitiva, la divulgación de las fotografías en que aparezcan personas reconocibles o identificables es una comunicación de datos, para la que sería necesario el previo consentimiento de las personas fotogra-

fiadas, salvo que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público.

A tal efecto se consideran buenas prácticas:

- Informar a la entrada del evento de la finalidad de la grabación de imágenes de las personas asistentes (mediante carteles o paneles informativos, folletos, entre otros) y su posterior difusión, incluyendo en la información la mención a la competencia de la Autoridad Vasca de Protección de Datos.
- Si se cursa invitación se debe advertir de que la Universidad tomará fotografías y/o grabará vídeos para una eventual y posterior difusión.
- Las y los profesionales encargados de la captación de material audiovisual deberán portar algún elemento distintivo que los distinga para permitir a las personas reconocer a dichos profesionales para, en su caso, rechazar la captación de su imagen.
- En todo caso, las y los fotógrafos oficiales centrarían la captura de imágenes y vídeos del evento en tomas generales de las personas asistentes, de forma que ninguna adquiera un papel exclusivo o predominante y la presencia de cualquiera de ellas pueda entenderse como accesoria, evitando en la medida de lo posible la captación frontal de la persona que permita su identificación.

Obtención de material audiovisual en un acto universitario por parte de particulares

Las grabaciones y toma de fotografías de las imágenes de familiares que participan en eventos universitarios se encuentran amparadas en el ámbito personal y doméstico y, por tanto, excluido de la aplicación del RGPD en la medida en que las imágenes sean tomadas por particulares para sus fines privados y familiares, siendo en todo caso responsables de su tratamiento las personas que toman dicho material.

A tal efecto, constituye una buena práctica informar mediante paneles o carteles informativos a las personas asistentes de que asumen en exclusiva la responsabilidad que se derive de la captación y difusión del material audiovisual que capten.

Grabación de imágenes en instalaciones deportivas de la Universidad

La captación de imágenes de las personas que se entrenan en estas instalaciones no constituye un evento público de modo que su grabación claramente conllevaría la captación continua y no accesoria de las imágenes de las personas que los efectúan y que pueden tener al respecto unas justificadas expectativas de privacidad, por lo que requerirían consentimiento de la persona.

Videovigilancia por razones de seguridad

La videovigilancia por razones de seguridad tiene como finalidad la protección y seguridad de personas, instalaciones y bienes de la UPV/EHU ante la eventual causación de daños y perjuicios tanto a personas como a propiedades de la institución frente a acciones que pudiera realizar el personal y alumnado vinculado a la institución de forma intencionada o negligente.

En la grabación de imágenes por razones de seguridad sólo podrán captarse imágenes de espacios interiores y de la vía pública en la medida en que resulte imprescindible para la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones. En ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado. La zona objeto de videovigilancia será la mínima imprescindible abarcando espacios públicos como accesos o pasillos.

No podrán instalarse en espacios protegidos por el derecho a la intimidad como aseos, vestuarios o aquellos en los que se desarrollen actividades cuya captación pueda afectar a la imagen o a la vida privada como los gimnasios.

No se considera razonable utilizar esas cámaras con fines de control de asistencia a clase, al existir otros medios menos intrusivos o invasivos de la intimidad.

La presencia de dispositivos de videovigilancia será advertida mediante carteles informativos ubicados anticipadamente al espacio de captación de dichos dispositivos.

9. Seguridad y garantía en el tratamiento de datos personales de la UPV/EHU

Seguridad en las actividades de tratamiento de datos personales

La UPV/EHU, como institución integrada en el sector público, garantiza el cumplimiento del Esquema Nacional de Seguridad en todas sus actividades de tratamiento de datos personales.

El responsable de la información, según el Esquema Nacional de Seguridad, se corresponde con el responsable del tratamiento definido en el Reglamento general de protección de datos.

El responsable del servicio, el responsable de seguridad y el responsable de sistemas, junto con las y los administradores de seguridad y el resto de personal técnico velarán por el establecimiento y mantenimiento de las medidas técnicas, humanas y organizativas que permitan realizar las actividades de tratamiento de datos personales con las garantías exigibles en la normativa vigente.

Seguridad y confidencialidad de la información

Los datos serán tratados de forma confidencial y estarán sometidos a medidas técnicas y organizativas de seguridad adecuadas para evitar su alteración, pérdida, tratamiento o acceso no autorizado a cuyos efectos se actuará conforme a los procesos internos de seguridad adoptados por la Universidad.

Todo el personal de la UPV/EHU y quienes intervengan en cualquier fase del tratamiento de los datos personales están obligados a guardar confidencialidad respecto de los datos personales a que tengan acceso y conocimiento, aún después de finalizar su relación con la institución.

Asimismo, la institución puede desarrollar normas internas de uso de los recursos informáticos y de comunicaciones en garantía de la seguridad y protección de los datos personales requeridos por la legislación vigente y que se enmarcan en la política de seguridad de la información y sus procedimientos se incorporarán al sistema de gestión de seguridad de la información.

Seguridad en los equipos y sistemas de información que traten datos personales

La UPV/EHU dispone de políticas y procedimientos específicos para definir un nivel de seguridad equivalente en el caso de equipos y dispositivos de terceras partes que se deban integrar o utilizar los recursos de la UPV/EHU, como en el caso de personal que utilice equipamiento propio para realizar sus funciones o dispositivos conectados a la red de la Universidad

Todos estos recursos se encuentran adecuadamente administrados y configurados impidiéndose el acceso o uso no autorizado.

Garantía de los derechos digitales en el uso personal de recursos corporativos

Los recursos informáticos y la información que contienen son utilizados únicamente para actividades de producción, desarrollo, investigación, docencia y gestión administrativa relacionadas con la UPV/EHU y de forma que no interfieran la actividad de las personas miembros de la comunidad universitaria.

La cuenta corporativa de correo electrónico y los servicios digitales que proporciona la UPV/EHU a toda la comunidad universitaria con quien tiene vínculo activo son herramientas profesionales o corporativas cuya titularidad recae en la institución.

Toda la información generada por las personas con vínculo activo en el desempeño de sus funciones debe ubicarse en el sistema de información y herramientas corporativas de la UPV/EHU.

Garantías de seguridad

Cada persona con acceso autorizado al sistema de información debe garantizar la seguridad en el acceso y uso del sistema de información aplicando medidas de seguridad técnicas y medidas organizativas apropiadas desarrollando con diligencia y con ayuda del Delegado de Protección de Datos la actividad necesaria para los propósitos que se indican a continuación.

1. Preservar la confidencialidad respecto de la información personal conocida con motivo del ejercicio de las tareas.
2. Trasladar nuevos tratamientos que deban identificarse en el Registro de actividades de Tratamiento, nuevas actividades de un tratamiento ya registrado o discrepancias entre la realidad de la forma de actuar y lo recogido en el Registro-
3. Guardar la documentación o aplicativo que refleja el cumplimiento del deber de información y, en su caso, los consentimientos firmados en los casos en que deban recogerse,
4. Informar adecuadamente a las personas en relación al tratamiento de sus datos personales.
5. Recopilar los compromisos firmados de confidencialidad en casos en que se requiera de forma específica,
6. Dar acceso de los expedientes a las personas interesadas debiendo distinguirse entre el acceso administrativo al expediente, el acceso al expediente derivado del ejercicio de derechos vinculados al tratamiento de datos personales, el acceso por transparencia o el acceso por requerimiento de autoridades o instituciones públicas en el ejercicio de sus competencias.

7. Responsabilizarse del cuidado de la información personal de las personas cuyos datos se tratan.
8. Ponerse en contacto y/o a disposición del Delegado de Protección de Datos para realizar los análisis de los riesgos del tratamiento de datos personales y, en su caso, evaluaciones de impacto.
9. Participar en las actividades formativas establecidas por la UPV/EHU en materia de protección de datos personales y seguridad de la información.
10. Trasladar a la organización las incidencias de seguridad que se detecten en el tratamiento de datos automatizado o no automatizado en aras a documentar las violaciones o brechas de seguridad y garantizar la comunicación a las personas afectadas y la notificación a la Agencia Vasca de Protección de Datos, en caso en que se valore necesario efectuar dicha comunicación y notificación.

Análisis de Riesgos

Cada área o servicio debe analizar, con la ayuda del Delegado de Protección de Datos, las actividades que desempeña, su naturaleza, el contexto en el que se desarrolla y su finalidad para conocer y, en su caso, detectar los riesgos posibles de que un impacto negativo, sobre los datos personales afecte a la confidencialidad entendida como la capacidad de la información de no ser revelada a personas no autorizadas, a la integridad o capacidad de la información de no ser alterada y conservar su exactitud y la disponibilidad o accesibilidad de la información para las personas autorizadas. Propiedades de la información que quedan comprometidas en circunstancias tales como pérdida, robo, revelación o inaccesibilidad.

El análisis de riesgos consiste en analizar las probabilidades de que pueda verse afectada alguna de esas tres propiedades planteándose la hipótesis o escenarios de que personas no autorizadas accedan a los datos, que estos sean manipulados indebidamente de forma accidental o deliberada o que no se pueda acceder a los datos.

En la UPV/EHU el Análisis de Riesgos se realiza con el DPD, previamente a la inclusión del tratamiento en el Registro de Actividades de Tratamiento (RAT) de modo que cada área completa un cuestionario del que se derivarán, en función a las respuestas, dicho análisis de riesgos. Dicho cuestionario se encuentra en Formulario para el registro de Tratamientos - Secretaría General - UPV/EHU

Evaluación de Impacto sobre la Protección de Datos (EIPD)

Si al realizar el análisis de riesgos se concluye que uno o varios tratamientos de datos conllevan un riesgo significativo o alto para la privacidad de las personas, la institución debe acometer una evaluación de impacto; es decir, un proceso sistemático con una metodología determinada para analizar los riesgos significativos que la gestión y tratamiento de datos puede comportar para la protección de los datos, los derechos y libertades de las personas titulares de dicha información personal.

10. La Autoridad Vasca de Protección de Datos

La Ley 16/2023, de 21 de diciembre, de la Autoridad Vasca de Protección de Datos ha supuesto una importante actualización de las obligaciones para las instituciones públicas vascas en materia de protección de datos. Comentaremos a continuación algunas de ellas.

Esta Ley adapta la organización y funcionamiento de la Autoridad Vasca de Protección de Datos, denominada antes como Agencia, determina las personas y entidades afectadas por ellas y detalla el régimen sancionador, como principales aspectos.

El objeto de la Ley es, según su propia definición, adaptar la organización y funcionamiento de la normativa aplicable a la Comunidad Autónoma del País Vasco a las previsiones del Reglamento (UE) 2016/679, de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, así como de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

Esta Ley es aplicable a los tratamientos de datos personales de los que sean responsables:

- las entidades del sector público autonómico foral y local del País Vasco, y
- el sector privado en los siguientes supuestos:
  - Cuando realicen funciones que sean competencia de las Administraciones Públicas de la comunidad autónoma,
  - Cuando los tratamientos los ejecuten las entidades privadas que prestan servicios públicos, mediante cualquier forma de gestión directa o indirecta al considerarse esos servicios como prestados por la administración pública titular, y
  - Cuando lo realicen entidades privadas que prestan servicios como encargadas del tratamiento a las administraciones y entidades públicas de la Comunidad Autónoma

Específicamente se refiere Universidad del País Vasco (UPV/EHU) y las demás universidades integrantes del Sistema Universitario Vasco, así como los entes de ellas dependientes. Además, contempla que la Autoridad concluirá acuerdos y convenios de colaboración con la Universidad del País Vasco (UPV/EHU), además de con las restantes universidades y entidades integrantes del Sistema Universitario Vasco y centros educativos no universitarios.

Esta Ley determina que están sometidos al régimen sancionador, entre otros, los responsables y encargados en los tratamientos sometidos al ámbito de aplicación de esta norma.

Cuando las administraciones, entidades e instituciones públicas vascas incluidas en el ámbito de aplicación de esta ley, actuando como responsables o encargados del tratamiento, cometiesen alguna de las in-

fracciones contempladas en ella, la Autoridad Vasca de Protección de Datos dictará resolución declarando la infracción y dirigiendo un apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

La resolución adoptada se notificará al responsable o encargado del tratamiento, así como, en su caso, al órgano del que dependa jerárquicamente, y a la persona denunciante

Además, la Autoridad Vasca de Protección de Datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades, altos cargos y personal directivo, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con la denominación del cargo que fuese responsable y se ordenará su publicación en el «Boletín Oficial del País Vasco».

Además, establece que se comunicarán al Ararteko las resoluciones sancionadoras dictadas.

El inicio del procedimiento incluye la admisión o inadmisión a trámite de la reclamación y las actuaciones previas enumerando una lista de supuestos de inadmisión; que la reclamación no verse sobre cuestiones de protección de datos personales, que carezca notoriamente de fundamento, sea abusiva o no aporte indicios racionales de la existencia de una infracción. Igualmente, la Autoridad Vasca de Protección de Datos podrá inadmitir a trámite la reclamación cuando el responsable o encargado del tratamiento, previa advertencia formulada por aquella, hubiera adoptado medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos y concurra alguna de las siguientes circunstancias, que no se haya causado perjuicio a la persona afectada en el caso de las infracciones con la consideración de leves a efectos de prescripción o que el derecho de la persona afectada quede plenamente garantizado mediante la aplicación de las medidas adoptadas.

También prevé que la autoridad acuerda iniciar el procedimiento cuando se lo requiera otra Autoridad de Protección de Datos, incluso la estatal, y hacerlo de oficio cuando conozca indicios de una infracción de la normativa de protección de datos.

11. Pautas para la gestión de los datos personales en la gestión académica y docente

A continuación, se incorpora un proceso de distintos hitos dirigidos a procurar una gestión adecuada en el tratamiento de datos personales que requiere la actuación y ejercicio de tareas y competencias.

Pautas de gestión de datos personales
1. Identificar si nuestra gestión requiere tratar datos personales
2. Determinar los usos permitidos de los datos personales
3. Aplicar el tratamiento de datos personales a una finalidad determinada
4. Definir el colectivo de personas afectadas por el tratamiento de datos personales
5. Informar a las personas acerca del tratamiento de sus datos personales
6. Analizar la presencia de categorías especiales de datos
7. Analizar la necesidad de comunicar o ceder datos personales a terceros
8. Verificar la existencia de transferencias internacionales de datos personales
9. Proteger el contexto espacial en la gestión de de datos personales
10. Garantizar el adecuado ejercicio de derechos relativos al tratamiento de datos personales

1. Identificar si nuestra gestión requiere tratar datos personales

La primera cuestión es ***determinar si la actividad que desempeñamos requiere tratar datos personales***. Por ejemplo, la gestión de la actividad docente y académica requiere gestionar datos personales del colectivo correspondiente al alumnado, pero no así la realización de encuestas relativas a la calidad del servicio que pueden y deben realizarse de forma anónima de modo que esta actuación no requiere tratar información personal.

A estos efectos, se entiende por datos personales cualquier información sobre una persona física identificada o identificable considerándose como tal a cualquier persona que pueda ser determinada, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de esta persona.

En sentido contrario, no es dato personal la información anonimizada, es decir, información que no guarda relación con una persona física identificada o identificable, ni los datos convertidos en anónimos de forma que la persona no sea identificable, o deje de serlo, aspecto que se desarrolla a continuación.

Tampoco serán datos personales la información desvinculada o no vinculada a una persona concreta, como los datos agregados, genéricos o estadísticos. Por ejemplo, el número de atenciones que se realizan en el servicio de atención al alumnado, las características del servicio prestado, la estadística de personas y su género atendidas en un campus y/o en un periodo concreto.

Para llegar a esta consideración debe analizarse cada supuesto por cuanto no es información anónima aquélla que, pese a eliminarse la identidad de las personas, pueda ser reconstruida y reidentificar a la persona a partir de la suma o combinación de datos que constan en un expediente.

2. Determinar los usos permitidos de los datos personales

La segunda actuación es ***determinar las posibles actuaciones de tratamiento de datos personales.***

Es tratamiento de datos personales cualquier operación realizada sobre datos personales por procedimientos automatizados o no automatizados, tales como la recogida, registro, organización, conservación, modificación, consulta, acceso, comunicación, entre otras actuaciones.

> Los datos personales serán mantenidos de forma que se permita la identificación de las personas durante el tiempo necesario para gestionar las actividades del tratamiento y de acuerdo con sus finalidades. Y serán suprimidos cuando hayan dejado de ser necesarios. La supresión no implica la destrucción sino el bloqueo de los datos para dar respuesta ante reclamaciones, requerimientos o responsabilidades y durante el período de tiempo en el que dichas acciones puedan ejercerse conforme a la norma que sea de aplicación. Ello sin perjuicio de conservar la información durante períodos largos por motivos de archivo en interés público, fines de investigación científica e histórica o fines estadísticos.

En el Registro de Actividades de Tratamiento relativo a la gestión se reseña el período de conservación de la información aplicable por la UPV/EHU a cada tratamiento que comprende la gestión académica y docente, Registro que, como ha quedado indicado, se encuentra disponible en que se encuentra disponible en https://www.ehu.eus/es/web/idazkaritza-nagusia/babestu

3. Aplicar el tratamiento de datos personales a una finalidad determinada

Los usos o finalidades del tratamiento de los datos personales; esto es, qué se puede hacer con esta información, no son aleatorios ni quedan a la elección de la persona que los gestiona en ejercicio de sus competencias laborales y profesionales, sino que están diseñadas y contenidas en el ***Registro de Actividades de Tratamiento (RAT)*** de la UPV/EHU disponible en https://www.ehu.eus/es/web/idazkaritza-nagusia/babestu

El RAT supone un análisis de las actividades de tratamiento que efectúa una organización valorando aspectos relativos a la forma de tratar y gestionar los datos, estableciendo para qué pueden ser utilizados (finalidad), qué datos han de recabarse (necesidad y proporcionalidad), a qué colectivos de personas afecta, cuál es el origen o procedencia de dichos datos, el título jurídico que permite o habilita su (legitimación), el plazo para su conservación si van a ser comunicados a terceras personas u organizaciones destinatarias, si requiere transferencias internacionales de datos o las medidas de seguridad que los van a proteger.

Por lo tanto, conocer el contenido de este Registro facilitará al personal que trata datos personales en el ejercicio de su actividad conocer qué actividades de tratamiento de datos puede realizar y, de ese modo, saber qué se puede hacer o no en cada situación.

La consideración, decisión y responsabilidad de la elaboración y contenidos del RAT no recae en el personal sino en la organización en tanto responsable del tratamiento que dará a conocer a su personal este contenido para que lo aplique estrictamente, correspondiendo su realización y actualización a las áreas y/o servicios de la UPV/EHU. Así pues, las personas responsables de las distintas áreas y negociados que desarrollen actividades que impliquen el uso de datos personales, deberán valorar si dicho tratamiento se encuentra recogido en el RAT publicado por la Universidad (BABESTU), y en su caso, rellenar el formulario de declaración de un tratamiento nuevo conforme al contenido dispuesto en https://www.ehu.eus/es/web/idazkaritza-nagusia/tratamenduak-erregistratzeko-formularioa

4. Definir el colectivo de personas afectadas por el tratamiento de sus datos personales

El tratamiento de los datos se proyecta sobre personas físicas siendo necesario determinar a qué colectivo pertenecen.

Por ejemplo, la gestión docente se efectúa sobre el colectivo de personas que conforman el alumnado, sin embargo, en su gestión académica es usual que concurran datos de terceras personas principalmente padres, madres, personas progenitoras y tutoras cuyos datos identificativos y de contacto son necesarios, por ejemplo, para comunicar la situación académica del alumno o alumna conociendo en qué escenarios esta comunicación de datos puede producirse.

Este escenario tiene una doble valoración: (1) determinar si se van a tratar los datos directamente de las personas interesadas, y (2) determinar si el tratamiento requiere conocer y gestionar datos de terceras personas vinculadas a la interesada, por cuanto en ambos casos es necesario gestionar la información a las personas de una forma concreta.

5. Informar a las personas acerca del tratamiento de sus datos personales

Quién debe informar y cuándo

La obligación de informar a las personas en el momento de la recogida, sobre los aspectos referentes al tratamiento de sus datos corresponde a la UPV/EHU como responsable del tratamiento sin perjuicio del formato en el que materializar la información. Por ejemplo, en el momento de realizar la matrícula a través del formulario establecido al efecto.

De qué debe informarse a la persona titular de datos personales

La información a las personas acerca de qué y para qué se van a tratar sus datos personales es una obligación previa a la recogida de datos personales.

Presentación de la información por capas o niveles

La LOPDGDD introduce este concepto de información por capas o niveles, refiriéndose a cómo presentar la información a la persona a la que solicitas los datos.

Primera capa o primer nivel de información: fragmento informativo

El contenido básico de la información que UPV/EHU da a la persona se corresponde con la llamada «primera capa» o «primer nivel de información», consistiendo en un fragmento informativo que suele figurar en formularios en formato papel u on line y que debe contener los siguientes aspectos:

1. Responsable del tratamiento: UPV/EHU
2. Actividades de tratamiento y código del tratamiento (código que figura en el Registro de Actividades de Tratamiento RAT) que está disponible a efectos informativos en https://www.ehu.eus/es/web/idazkaritza-nagusia/babestu
3. Modo de acceder a la información adicional y a cómo ejercer los derechos relativos al tratamiento de los datos personales.

Por ejemplo, un formulario de inscripción o de matriculación contendrá un fragmento informativo breve limitado a indicar a la UPV/EHU como responsable de tratamiento, la finalidad -breve- para la que se recaban los datos personales solicitados y una indicación del punto informativo donde obtener información adicional sobre dicho tratamiento y cómo poder ejercer los derechos relativos a la gestión de datos personales, por ejemplo mediante un link o vínculo o referencia al apartado de babestu donde figura el Registro de Actividades de Tratamiento.

Segunda capa o segundo nivel información: información adicional

Este segundo nivel e se corresponde con el contenido detallado e los tratamientos de datos personales efectuados por UPV/EHU que se recoge en su Registro de Actividades del Tratamiento.

Forma

Así, en las instrucciones para rellenar el formulario de declaración de un tratamiento nuevo a que se ha hecho referencia https://www.ehu.eus/es/web/idazkaritza-nagusia/tratamenduak-erregistratzeko-formularioa se indica cómo ha de completarse el fragmento informativo de primera capa y la información detallada:

> **18. Información legal básica (1ª capa)**
>
> A partir de toda la información que pacientemente ha suministrado en este formulario, en este punto se puede obtener la información mínima que debe suministrar a las personas interesadas en el momento de recabar sus datos personales o informarles de su tratamiento. Es una INFORMACIÓN MÍNIMA Y OBLIGATORIA. Puede imprimirla, copiarla por los medios informáticos a su alcance, pero no puede obviarla.

> **19. Información legal completa (2ª capa)**
>
> Es este punto puede obtener la información completa que las personas interesadas pueden consultar. Se albergará en una página web referenciada en el punto 18, pero es recomendable que se suministre en primera instancia, si ello es posible.

6. Analizar la presencia de categorías especiales de datos

El tratamiento de los datos requiere de actuaciones de mayor exigencia y control y, en definitiva, de mayor protección, cuando concurren datos especialmente sensibles, a los que la normativa denomina categorías especiales de datos por poseer una particular afectación a la intimidad y privacidad de las personas de modo tal que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales de la persona a quien corresponden.

Los datos especialmente protegidos que integran la denominada categoría de datos especiales son los relativos a:

- Origen étnico o racial
- Opiniones políticas
- Convicciones o creencias religiosas o filosóficas
- Afiliación sindical
- Datos de salud
- Datos genéticos
- Datos biométricos dirigidos a identificar de manera unívoca a una persona, y
- Datos relativos a la vida sexual u orientación sexual

Además, hay un conjunto de datos que se consideran de mayor relevancia que los básicos u ordinarios por su particular sensibilidad pero que no constituyen categorías especiales de datos, considerándose datos especialmente sensibles siendo estos los relativos a:

- Violencia de género
- Datos relativos a condenas y delitos penales
- Datos relativos a sanciones administrativas, y
- Datos de personas de colectivos en situación de especial vulnerabilidad como personas menores de edad, discapacitadas, de avanzada edad, en riesgo de exclusión social, personas en situaciones políticas comprometidas, sin papeles, u otros supuestos vulnerables por su situación más frágil a considerar el riesgo del tratamiento de sus datos personales.

7. Analizar la necesidad de comunicar o ceder datos personales a terceros

Para la normativa de protección de datos es cesión o comunicación de datos la revelación de datos realizada a una persona distinta de la persona interesada.

A este respecto, la gestión universitaria requiere en muchas ocasiones la participación o intervención de terceras personas u organizaciones públicas y /o privadas ajenas al ámbito de la UPV/EHU a las que se ceden o comunican datos.

Es el caso de la participación de personas colaboradoras, de otras instituciones académicas públicas o privadas, de organismos públicos, que bien por el cumplimiento de obligaciones legales impuestas a la Universidad como por el ejercicio de competencias públicas correspondientes a ésta requieren de la intervención de terceros. Para conocer qué cesiones se pueden o deben realizar debe acudirse el Registro de Actividades de Tratamiento de la UPV/EHU que las refleja.

Además, la propia gestión de la organización requiere de la prestación de servicios de terceras organizaciones, proveedoras externas de servicios, que requiere la UPV/EHU para desarrollar su gestión, y que integran la cualidad jurídica, a efectos de la normativa de protección de datos, de encargadas de tratamiento. Por ejemplo: prestación de gestorías laborales, proveedoras de facturación electrónica o servicios informáticos externos.

En estos escenarios de provisión de servicios, no estamos ante una cesión de datos propiamente dicha, sino de servicios que la Universidad provee a través de terceros de modo tal que la comunicación de datos o acceso a estos es necesario para la prestación del servicio a modo de extensión de la gestión de la organización que ésta no puede desarrollar por sí misma, conservando ésta la condición de responsable del tratamiento.

En tales casos de provisión de servicios la UPV/EHU formalizará un ***contrato de encargo de tratamiento*** con la organización (persona jurídica) o profesional autónomo por el cual quien provee del servicio se obliga al cumplimiento de la normativa de protección de datos, con obligaciones específicas que deben recogerse en dicho contrato.

8. Verificar la existencia de transferencias internacionales de datos personales

La normativa de protección de datos personales ha establecido tradicionalmente que la salida de los datos de las fronteras de la Unión Europea plantea algunos riesgos añadidos, riesgos que son inasumibles por las personas titulares de dicha información salvo que hayan emitido su consentimiento para este tránsito de datos personales y a tal efecto el Reglamento Europeo distingue varias situaciones:

- Los datos pueden transferirse a otros Estados de la Unión europea (mismo marco de protección)
- Los datos pueden transferirse a Estados que cuentan con una decisión de adecuación (Estados seguros).
- La transferencia de datos personales a Estados Unidos tiene una especial consideración existiendo tradicionalmente acuerdos especiales para el desplazamiento de los datos, no a la totalidad del país sino a organizaciones específicas estadounidenses, conforme a acuerdos con la Unión Europea en vigor en cada momento.
- Transferencia a terceros estados que no están en ninguna de las situaciones precedentes.

Es muy habitual en la prestación de servicios por las organizaciones públicas y privadas que servicios colaterales o auxiliares necesarios para dicha prestación, incluso gratuitos, se efectúen por empresas extranjeras ubicadas fuera del Espacio Económico Europeo de modo que la prestación del servicio suponga el desplazamiento de los datos a dichos Estados. O que, aunque esas proveedoras se encuentren dentro de la Unión Europea se provean a su vez de servicios técnicos para la prestación del servicio o de alojamiento de datos, que no se encuentran dentro de dicho Espacio.

Por ello, las organizaciones deben analizar, auditar y garantizar un nivel de protección adecuado revisando que sus proveedoras de servicios con hostings, alojamientos, servicios de procesamiento, servidores o servicios técnicos cumplan con lo exigido por la normativa europea de protección de datos por lo que a la consideración e implicaciones, de transferencias internacionales respecta, debiendo realizarse únicamente transferencias de datos personales a un tercer país u organización internacional atendiendo a las condiciones establecidas en la normativa de protección de datos.

9. Proteger el contexto espacial en la gestión de datos personales

El contexto espacial en que se desarrollan las tareas que requieren la gestión y almacenamiento de datos personales es un aspecto vinculado a la confidencialidad y se relaciona estrechamente con la confianza de las personas de que sus datos serán tratados adecuada y respetuosamente.

Es para ello necesario mantener actitudes que garanticen preservar la documentación en papel debidamente protegida, así como cerrar o bloquear la sesión cuando dejen de ser utilizados.

Constituye una buena práctica de política de mesas limpias, al abandonar el puesto de trabajo con motivo de una ausencia temporal correspondientes a descansos, pausas o similares o fin de la jornada laboral, dejar libre de documentación el puesto de trabajo, usando archivadores, cajoneras o armarios y haciendo uso de sus dispositivos de cierre, así como prestar atención a que no quede documentación en las impresoras o pendiente de imprimir.

No deben dejarse a mano de terceras personas que puedan acceder a ellos documentos en papel y se impedirá la visualización del contenido de las pantallas.

Se recomienda no reutilizar o destruir el papel que contenga datos de carácter personal (modelos, listados, etc.).

Asimismo, no se debe copiar la información contenida en el sistema de información en los que se almacenan datos de carácter personal a cualquier soporte USB o dispositivos externos o listados en papel), ni extraerla del puesto de trabajo centro salvo en casos de necesidades del servicio que la organización haya determinado y autorizado que requieren dicha salida.

10. Garantizar el adecuado ejercicio de derechos relativos al tratamiento de datos personales

La normativa de protección de datos contempla un conjunto de derechos que garantiza a las personas el poder de control sobre sus datos personales y que la UPV/EHU en tanto responsable del tratamiento debe garantizar.

Se trata de derechos cuyo ejercicio es personalísimo, de modo tal que sólo pueden ser ejercitados por la persona titular de los datos, por su representante legal o por otra persona física que acredite ostentar su representación.

- **Acceso:** derecho a obtener información del tratamiento de datos.
- **Rectificación:** derecho a actualizar los datos inexactos o incompletos.
- **Supresión:** derecho a eliminar los datos.
- **Limitación:** Derecho que consiste en el marcado de datos para restringir parte del tratamiento que se está realizando.
- **Oposición:** Derecho a no proseguir con el tratamiento de datos.
- **Portabilidad:** Derecho a obtener una copia para la transmisión de datos a otra proveedora de servicios o a la propia persona interesada.
- **Derecho a no ser objeto de decisiones individuales automatizadas:** Derecho oponerse a un tratamiento cuya finalidad sea adoptar decisiones individuales destinadas a evaluar, analizar o predecir aspectos personales con efectos jurídicos para la persona.

En la UPV-EHU el canal ante de recepción de solicitudes para el ejercicio de derechos en esta materia es dpd@ehu.eus

Además, si la persona solicitante cree que sus derechos en esta materia no han sido atendidos en forma y plazo, o la respuesta es insatisfactoria, puede recabar la tutela de las autoridades de control que en el caso del sector público vasco, en que se encuadra la institución universitaria de la UPV/EHU es la Autoridad Vasca de Protección de Datos (AVPD). La autoridad Vasca de Protección de Datos se encuentra regulada en la Ley 16/2023, de 21 de diciembre, de 21 de diciembre, de la Autoridad Vasca de Protección de Datos, que establece en su artículo 2.1.j) la competencia de la Autoridad y la aplicación de la ley a la Universidad del País Vasco así como al resto de Universidades del sistema universitario vasco.