POLÍTICA DE PROTECCIÓN DE DATOS

Aprobada por el Consejo de Gobierno de 10 de marzo de 2022

I. ANTECEDENTES Y OBJETIVOS DE LA POLÍTICA

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental consagrado en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea y en el artículo 18.4 de la Constitución Española. Con la aprobación del Reglamento (UE) del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante "RGPD") y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, "LOPD"), y atendiendo al carácter dinámico de las Políticas de Protección de Datos se hace necesario realizar una revisión de las bases jurídicas de la protección de datos de carácter personal con la finalidad de proteger y salvaguardar dicho derecho.

Así, la UNIVERSITAT POLITÈCNICA DE VALÈNCIA (en adelante "la UPV") como institución de derecho público de educación superior, dirigida a, entre otras funciones, a formar a personas para potenciar sus competencias, investigar y generar conocimiento con el objetivo de impulsar el desarrollo integral de la sociedad y contribuir a su progreso tecnológico, económico y cultural, está comprometida con la protección de los datos de carácter personal de los que es responsable o encargado de tratamiento.

Con la implantación de la Administración Electrónica que garantiza la trazabilidad en el tratamiento de los datos, su seguridad e integridad, así como las Políticas desarrolladas en los últimos tiempos, la UPV se ha ido adaptando a los distintos cambios normativas aprobados en la materia.

En cumplimiento de dicha normativa, se ha designado un Delegado de protección de datos que tiene como funciones, la supervisión del cumplimiento del Reglamento General de Protección de Datos y de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales en el ámbito de la UPV, la supervisión de las políticas de privacidad del responsable del Tratamiento en el ámbito de la UPV, así como la cooperación con la autoridad de control correspondiente. Dicho nombramiento ha sido comunicado a la Agencia Española de Protección de Datos.

Asimismo, se ha aprobado el Reglamento del Registro de Actividades de Tratamiento de la UPV que derogó el Reglamento sobre Protección de Datos de Carácter Personal de la Universidad Politécnica de Valencia del año 2010, elaborándose asimismo un Registro de Actividades de Tratamiento, accesible en la web de la UPV para que todos tengan conocimiento de los tratamientos de datos personales que se realizan. Se ha aprobado la Política de Seguridad en el marco del Esquema Nacional de Seguridad, designándose al responsable de seguridad de la Información y al Comité de Seguridad TIC de la UPV y se ha atendido al ejercicio de derechos de los distintos usuarios de la Universidad, entre otras actuaciones.

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen

Por ello esta política tiene como objetivo actualizar los principios que rigen en la Universidad de forma que se garantice el cumplimiento de la legislación aplicable en dicha materia tras los cambios normativos aprobados, así como garantizar los derechos y libertades de los interesados mediante la adopción de diversas medidas de seguridad. Conforme a dichos objetivos, se ha desarrollado un Sistema de Gestión de Protección de Datos (SGPD) que permita dar cumplimiento a los requerimientos establecidos en el RGPD y la LOPD, como también mejorar de forma continua los procesos que dan soporte al tratamiento de datos de carácter personal.

II. ÁMBITO DE APLICACIÓN

La presente Política se aplicará a todos los sistemas de información y a todas las actividades de tratamiento de datos de carácter personal de los que sea responsable la UPV.

Será de obligado cumplimiento para todos los órganos superiores y directivos de la UPV, así como para todo el personal que acceda, tanto a los sistemas de información, como a la propia información de la que es responsable la UPV, con independencia de cuál sea su destino, adscripción o relación con el mismo. Así, es obligatoria para todas las partes interesadas, ya sean internas o externas, que mantengan cualquier tipo de relación con la universidad y que, además, en el ejercicio de sus actividades, participen de forma directa o indirecta en el tratamiento de datos de carácter personal, siendo la Universidad la principal interesada y por ello comprometida en cumplir la Política.

III. PRINCIPIOS DE ACTUACIÓN

La UPV y todas las personas incluidas dentro del ámbito de aplicación de la presente Política se comprometen a:

1. Alcance estratégico: la protección de datos y la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos, de forma que se coordine e integre con el resto de las iniciativas estratégicas de la UPV.

2. Comunicar al Delegado de protección de datos: con carácter previo a su implantación, cualquier nueva actividad de tratamiento o cambio en las actuales que se pretenda llevar a cabo.

3. Respetar los principios relativos al tratamiento, utilizando los datos personales de una manera lícita y leal. Además, los datos que se recaben serán los adecuados, pertinentes y limitados a lo necesario para la finalidad para la que son recabados y no se destinarán posteriormente a otra finalidad incompatible.

4. Informar y, cuando sea obligatorio, recabar el consentimiento de los afectados. Por tanto, cuando resulte preciso solicitar y tener acceso a datos personales, confirmar que los interesados han recibido la correspondiente información de protección de datos y, en su caso, han prestado su consentimiento. La obligación de informar a las personas interesadas sobre

las circunstancias relativas al tratamiento de sus datos recae sobre el responsable del tratamiento, es decir sobre la UPV.

Los procedimientos de recogida de información pueden ser muy variados y, en consecuencia, los modos de informar a las personas interesadas deben adaptarse a las circunstancias de cada uno de los medios empleados para la recopilación o registro de los datos.

Así, la UPV informará a las personas interesadas con lenguaje claro y sencillo, de forma concisa, transparencia, inteligible y de fácil acceso.

La información se pondrá a disposición de los interesados en el momento en que se soliciten los datos, previamente a la recogida o registro, si es que los datos se obtienen directamente del interesado.

En el caso de que los datos no se obtengan del propio interesado, por proceder de alguna cesión legítima, o de fuentes de acceso público, el responsable informará a las personas interesadas dentro de un plazo razonable, pero, en cualquier caso:

- antes de un mes desde que se obtuvieron los datos personales,
- antes o en la primera comunicación con el interesado,
- antes de que los datos, en su caso, se hayan comunicado a otros destinatarios.

Esta obligación se cumplirá sin necesidad de requerimiento alguno, y la persona responsable deberá poder acreditar con posterioridad que la obligación de informar ha sido satisfecha.

1. Mantener los datos exactos y actualizados por el tiempo que dure la finalidad que justifica su tratamiento y, en todo caso, suprimirlos en el plazo que se considera prudente en atención a los distintos plazos de prescripción que pudieran afectar a la documentación que contenga los datos personales objeto de tratamiento.

2. Atender de un modo diligente y dentro del plazo legalmente establecido al ejercicio de los derechos que corresponden a cualquier interesado y a poner en marcha los mecanismos precisos para garantizar los derechos digitales en el ámbito laboral.

La normativa vigente en materia de protección de datos establece condiciones concretas sobre el procedimiento a seguir para atender a los interesados en el ejercicio de sus derechos, conteniendo en el artículo 12 del RGPD y LOPD-GDD algunas reglas comunes a su ejercicio.

Se arbitrarán fórmulas para facilitar al interesado el ejercicio de sus derechos en virtud de la citada normativa, incluidos los mecanismos para solicitar y, en su caso, obtener de forma gratuita, en particular, el acceso a los datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición. El responsable del tratamiento proporcionará medios para que las solicitudes se presenten por medios electrónicos, en particular cuando los datos personales se tratan por medios electrónicos.

Es por ello, que se ha decidido elaborar un procedimiento de ejercicio de derechos mediante el cual se cumpla con las obligaciones dispuestas en el RGPD y la LOPD-GDD en lo que respecta a los derechos de los interesados. Dicho procedimiento se encuentra publicado en el siguiente enlace https://www.upv.es/entidades/DPD/

1. Guardar confidencialidad y cumplir las medidas de seguridad que indique el r responsable de la seguridad de la Información.

2. Notificar cualquier brecha de seguridad: al responsable de seguridad y al delegado de protección de datos.

Un incidente de seguridad puede venir a través de fuentes internas a la organización (notificaciones de usuarios, alertas de antivirus, avisos de herramientas de monitorización, etc.) o fuentes externas (comunicación de un proveedor, clientes, INCIBE, CCN, Fuerzas y Cuerpos de Seguridad del Estado, medios de comunicación, etc.), y a su vez, tener múltiples implicaciones.

La violación de seguridad a la que se refiere el RGPD, aun siendo un incidente de seguridad, solo se aplica en la medida en que afecte a los datos de carácter personal.

Por ello, en el momento en que se identifique un incidente de seguridad, además de ser tratado de acuerdo al procedimiento dispuesto para ello, se comunicará al Delegado de protección de datos, para que tenga constancia debido a las posibles implicaciones que se deriven en cuanto al impacto sobre datos personales.

En base a la información obtenida, si el incidente ha tenido un impacto, o posible impacto, sobre datos de carácter personal, será tratada como brecha de seguridad de datos de carácter personal, procediendo a:

- Notificarlo al Delegado de protección de datos de la Universidad.
- Notificarlo al Responsablede Seguridad de la Universidad.
- Registrarla en el registro de brechas de seguridad
- Aplicar, en paralelo, las siguiente fases:

  - Analizar y clasificar la brecha de seguridad.
  - Responder al incidente.
  - Notificarla a las personas implicadas.
  - Notificar a la AEPD en caso de que fuera necesario (72horas).

La UPV ha elaborado un procedimiento de notificación de brechas de seguridad en materia de protección de datos, mediante el cual se cumpla con lo dispuesto en la normativa vigente en materia de protección de datos y en la presente Política. Dicho procedimiento se encuentra publicado en https://www.upv.es/entidades/DPD/

1. Proporcionalidad: Se establecerán medidas de protección, detección y recuperación que resulten proporcionales a los potenciales riesgos y a la criticidad y valor de la información, de los tratamientos de datos personales y de los servicios afectados.

2. Compromisos de terceros: Con carácter previo a la contratación o externalización de un servicio, incorporar al contrato las cláusulas relativas a la protección de datos, que aseguren el cumplimiento de sus obligaciones por parte de las empresas contratistas de la UPV.

3. Someter a una revisión o auditoría externa las Políticas y Procedimientos aprobados en materia de protección de datos con la finalidad de examinar el cumplimiento de la normativa aplicable y de los compromisos asumidos en virtud de la misma con carácter bienal.

4. Formar y concienciar de la importancia del cumplimiento de la presente Política, así como de la normativa de protección de datos a todas aquellas personas que traten datos de carácter personal en el ámbito de la UPV. Para ello, el Delegado de protección de datos impartirá anualmente sesiones formativas y de concienciación atendiendo a las distintas áreas de gestión de la UPV.

5. Profesionalidad: La implantación y seguimiento de la Política será encomendada a personal cualificado, dedicado e instruido en la normativa de protección de datos y de seguridad de la información. El personal de la UPV encargado recibirá la formación específica necesaria para ello. La UPV exigirá que las organizaciones que le prestan servicios en esta materia cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

6. Respecto al análisis de riesgos, el cambio de paradigma que ha establecido la Unión Europea con el RGPD respecto a la legislación nacional en materia de protección de datos existente en España, implica que las organizaciones entiendan el cumplimiento de esta normativa como un proceso basado en la gestión de riesgos.

Esta gestión es dinámica, cambiante en el tiempo, en función de nuevas amenazas y vulnerabilidades en los sistemas de información, de nuevos cambios en los reglamentos y normativas, del contexto de la organización, etc. Esto obliga a una revisión continua de los tratamientos y sus riesgos asociados.

El RGPD establece la necesidad de que el responsable o el encargado de tratamiento evalué los riesgos inherentes al tratamiento de datos de carácter personal y aplique medidas para mitigarlos.

Las medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deben protegerse.

Al evaluar el riesgo en relación con la seguridad de los datos, se tendrán en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen

forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

Asimismo, El RGPD y la LOPD-GDD incluye entre los requerimientos y obligaciones para las organizaciones la necesidad de evaluar el impacto de las actividades de tratamiento en la protección de los datos personales, siempre y cuando sea probable que el tratamiento suponga un riesgo significativo para los derechos y libertades de las personas. Es por ello que en la UPV se debe llevar a cabo un análisis para determinar la necesidad de la realización de una Evaluación de Impacto de Protección de Datos (EIPD) para determinar si los nuevos tratamientos de datos o los ya iniciados, presentan alto riesgo para los derechos o libertades de los interesados, a fin de estar en condiciones de poder adoptar las medidas pertinentes para adecuar dichos tratamientos a las exigencias de la normativa vigente en materia de protección de datos.

IV. ROLES Y RESPONSABILIDADES

Para el correcto cumplimiento de la normativa vigente en materia de protección de datos y de la presente Política se designarán, teniendo en cuenta las definiciones de puestos de trabajo, las necesidades de la Universidad y los derechos y deberes del personal de la misma, los roles y responsabilidades que se consideren necesarios y relevantes para la mejora continua del Sistema de Gestión de Protección de Datos.

En la presente política se definen los siguientes roles:

1.1. Responsable del tratamiento

La UPV como responsable de tratamiento se compromete a:

- Cumplir con los principios relativos al tratamiento: principio de licitud, lealtad y transparencia en el tratamiento de datos personales, principio de minimización, principio de exactitud, principio de limitación del plazo de conservación, principio de integridad y confidencialidad, principio de responsabilidad proactiva.

- Cumplir con la prohibición de la recogida de datos personales de fuentes ilegítimas, de fuentes que no garanticen suficientemente su legítima procedencia o de fuentes cuyos datos hayan sido recabados o cedidos incumpliendo la ley.

- Deber de diligencia en la elección de encargados de tratamiento.

- Adoptar las medidas necesarias para garantizar y demostrar que los datos que trata el encargado de tratamiento por cuenta de UPV se realizan conforme a los requerimientos del RGPD y la LOPD-GDD, estableciendo las responsabilidades para ambas partes en el documento de contratación.

- Adopción de las medidas requeridas por la normativa vigente en materia de protección de datos en los tratamientos de datos de carácter personal que impliquen una transferencia

internacional de datos a destinatarios establecidos en países fuera del Espacio Económico Europeo.

- Facilitar a los interesados el ejercicio de los derechos de acceso, rectificación, supresión y portabilidad de los datos, de oposición y limitación del tratamiento.

- Proporcionar la debida información acerca del tratamiento de datos, conforme a lo establecido en el RGPD y la LOPD-GDD, a aquellos interesados de los que se obtengan datos de carácter personal ya se de forma directa o indirecta.

- Cumplimiento del secreto profesional, incluso una vez que la relación contractual finalice.

- Valoración del riesgo de los tratamientos que se realizan.

- Adopción de las medidas de seguridad necesarias para proteger los derechos y libertades de los interesados conforme al proceso de gestión de riesgos.

- Notificación de "violaciones de seguridad de los datos" a la Autoridad de Control pertinente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.

- Designación de un Delegado de protección de datos.

- Realizar una Evaluación de Impacto sobre la Protección de Datos con carácter previo a la puesta en marcha de aquellos tratamientos que sea probable que conlleven un alto riesgo para los derechos y libertades de los interesados.

- Mantener un registro de actividades de tratamiento como responsable y/o encargado de tratamiento.

- Colaboración con las Autoridades de Control pertinentes.

4.2. Delegado de protección de datos

El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las siguientes funciones:

- Establecer las directrices para la implantación del SGPD, coordinando la asignación de recursos y tareas asociadas.

- Elaborar procedimientos y normativas para la mejora continua del SGPD.

- Establecer las directrices para la elaboración y mantenimiento del Registro de Actividades de Tratamiento.

- Evaluar cambios sobre el SGPD que impacten en la organización.

- Coordinación de las auditorías de cumplimiento.

- Coordinar con el responsable de seguridad, la seguridad de la información de carácter personal y de los tratamientos de carácter personal, de acuerdo a lo establecido en la Política de Seguridad de la Universidad.

- Informar al responsable de seguridad de los incidentes de seguridad relacionados con los datos de carácter personal.

- Seleccionar y seguir junto con el responsable de seguridad de las medidas de seguridad a implantar.

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.

- Supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales.

- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el RGPD.

- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida las consultas previas.

  El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

4.3. Responsable de Unidades (en Departamentos, Institutos, Centros y Servicios)

Las personas que desempeñan la Dirección de los Departamento, Institutos y Centros, así como aquellas que desempeñan las jefaturas de servicio en el ámbito competente en materia de protección de datos tendrán las siguientes funciones:

- Cumplir con la política corporativa de protección de datos y coordinar su aplicación entre las personas de su que formen parte del equipo.

- Cumplir con los procedimientos desarrollados en el SGPD que le sean de aplicación y coordinar su aplicación entre las personas que forman parte del equipo.

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen

- Notificar al Delegado de protección de datos cualquier incidente o brecha de seguridad que pueda afectar a los datos de carácter personal.

Asistir de forma obligatoria a los cursos formativos y de concienciación que se organicen en materia de protección de datos.

4.4. Empleados/Personal

Todos los miembros de la UPV tienen la obligación de conocer y cumplir la Política y en concreto, deberán:

- Cumplir con la política corporativa de protección de datos.
- Cumplir con los procedimientos desarrollados en el SGPD que le sean de aplicación.
- Notificar a su responsable en materia de protección de datos cualquier incidente o brecha de seguridad que pueda afectar a los datos de carácter personal.
- Asistir de forma obligatoria a los cursos formativos y de concienciación que se organicen en materia de protección de datos.

La UPV designará formalmente y comunicará a los interesados los roles y responsabilidades anteriormente descritos, atendiendo a su categoría profesional. La UPV formará al personal en materia de protección de datos para que puedan cumplir la presente Política, así como el resto de normativa en materia de protección de datos y de seguridad de la información.

V. IMPLEMENTACIÓN

La UPV desarrollará y mantendrá actualizada la Presente Política y los procedimientos que se elaboren en ejecución de la misma.

El responsable de seguridad y el delegado de protección de datos, serán los encargados de implementar en los sistemas de información de la UPV, los controles y desarrollos informáticos que sean adecuados para garantizar el cumplimiento de la normativa interna de protección de datos y velarán por que dichos desarrollos estén actualizados en cada momento.

Lo anterior se entenderá, en todo caso, sin perjuicio de las responsabilidades que correspondan a otros órganos de la UPV.

VI. REVISIÓN Y ACTUALIZACIÓN DE LA POLÍTICA

El delegado de protección de datos será el encargado de que la implementación y el cumplimiento de la presente Política sea revisada periódicamente.

La monitorización de la Política incluye:

(i) los procedimientos de ejercicio de derechos y de notificación de brechas de seguridad

(ii) las revisiones periódicas de la efectividad de la formación de los empleados en lo que concierne a estas cuestiones,

(iii) reportes y registros de las incidencias relacionadas con la presente Política, y

(iv) la revisión de la adecuación de la Política a la Legislación vigente.

En todo caso, la Política de protección de datos debe ser monitorizadas, evaluadas y registradas adecuadamente por la UPV con carácter bienal.

VII. DECLARACIÓN DE CUMPLIMIENTO

La presente Política de protección de datos es de obligado cumplimiento para todo el personal de la organización, para lo cual, la UPV promoverá dicha política y proporcionará orientación y apoyo a la gestión de la seguridad de la información de carácter personal de acuerdo con los requisitos de su actividad docente, las leyes aplicables y normas pertinentes.

La UPV reaccionará de forma inmediata ante eventuales incumplimientos de lo establecido en esta Política, dentro de los parámetros establecidos en la legislación vigente.

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen