crue Universidades Españolas Secretarías Generales

Guía sobre la protección de datos personales en el ámbito universitario en tiempos del COVID-19

Dulce Mª. García Mella (Presidenta del Grupo de Trabajo de Delegados de Protección de Datos. Secretaria General. Universidad de Santiago de Compostela)

Carlos A. Gómez Otero (Secretario General Adjunto. Universidad Santiago de Compostela)

AUTORES

Mónica Arenas Ramiro (Universidad de Alcalá. **Coordinadora**)

Luis Cancela de la Viuda (Universidad Politécnica de Madrid)

David Díaz Lima (Universidad Alfonso X El Sabio)

José Julio Fernández Rodríguez (Universidad Santiago de Compostela)

José Pascual Gumbau Mezquita (Universitat Jaume I de Castellò)

Victoria Madrona Ortega (Universidad Pablo de Olavide)

Ricard Martínez Martínez (Universidades de Valladolid, Burgos, Salamanca La Laguna, y Politècnica de València)

Margarita Martínez Pais (Universidad de Sevilla)

José Paz Blanco (Universidad de Cádiz)

Javier Plaza Penadés (Universitat de València)

Luz María Puente Aba (Universidade da Coruña)

Raquel Sánchez Rodríguez (Universidad Francisco de Vitoria)

Julián Valero Torrijos (Universidad de Murcia)

Marc Vives Pizá (Universitat Pompeu Fabra)

Javier Zazu Ercille (Universidad Pública de Navarra)

Versión 1.3, 24 de abril de 2020

Índice

ABREVIATURAS

AEPD	Agencia Española de Protección de Datos
DPD	Delegado/a de Protección de Datos
ENS	Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
LOPDGDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
LOU	Ley Orgánica 6/2001, de 21 de diciembre, de Universidades
RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

1. Presentación de la Guía

Las universidades han venido trabajando a través de la CRUE de forma colaborativa y desinteresada en asuntos de máximo interés y para beneficio de todas ellas y de la sociedad a la que sirven. Buena muestra de ello es la elaboración de múltiples documentos, que han servido, y siguen sirviendo, para orientar la actuación de las universidades, y la realización de estudios en materias complejas.

Sin duda, una de ellas ha sido la puesta en práctica de la legislación de protección de datos personales en el ámbito universitario, al ser las universidades entidades con múltiples especificidades y diversidad de actividades, muchas de ellas en vanguardia, para las que el ordenamiento jurídico no siempre ofrece una respuesta clara.

A la complejidad de dar cumplimiento a la legislación de protección de datos personales en la actividad ordinaria de las universidades, se ha añadido la situación excepcional derivada de la pandemia por COVID-19, que de la noche a la mañana ha cambiado los modelos tradicionales de la universidad presencial, pasando del trabajo en clase o despacho al trabajo online desde casa, con nuevos sistemas de docencia, nuevos modelos de evaluación y la priorización de actividades de investigación en el ámbito de salud y biomédico, especialmente sensible desde el punto de vista del tratamiento de los datos personales.

En este contexto el análisis de la aplicación de la normativa de protección de datos personales y garantía de los derechos digitales en las universidades debe partir de la idea-fuerza inicial de que el estado de alarma no ha limitado ni suspendido estos derechos, que mantienen toda su vigencia.

Debemos ser conscientes de que el derecho fundamental a la protección de datos se mantiene en el estado de alarma. Este derecho está totalmente operativo y es plenamente aplicable: la regulación del estado de alarma no permite suspender derechos fundamentales; y la normativa extraordinaria aprobada ahora ante la pandemia no restringe ni limita este derecho de protección de datos.

Tampoco han sido derogadas ni suspendidas de aplicación normas universitarias como la Ley Orgánica de Universidades, el Estatuto del Empleado Público, el Estatuto de los Trabajadores, el Estatuto del Estudiante Universitario o los Estatutos de cada una de las universidades, por lo que esta normativa universitaria debe ser interpretada siempre en favor del mantenimiento de los derechos y obligaciones de la comunidad universitaria.

Dicho esto, es preciso tener en cuenta también que la regulación de protección de datos permite adoptar medidas específicas frente a pandemias y necesidades de emergencia sanitaria, que se relacionan con habilitaciones legales ya existentes previamente, vinculadas a la protección de intereses vitales, interés público esencial, fines de medicina preventiva o laboral, diagnóstico médico, asistencia sanitaria o salud pública.

A iniciativa de un grupo de Delegados y Delegadas de protección de datos (DPDs) de varias universidades, a través de la CRUE se ha realizado una consulta a las universidades para identificar aquellos aspectos de la protección de datos que suscitan mayor preocupación en el actual estado de alarma. De esta consulta se han extraído las cuestiones que son objeto de tratamiento en esta guía, elaborada por una Comisión del Grupo de Trabajo de Protección de Datos de la Comisión Sectorial CRUE-Secretarías Generales que, con esfuerzo y dedicación, han conseguido que esté disponible en un corto período de tiempo. Dejamos aquí señalado también nuestro especial agradecimiento a CRUE-TIC cuyas aportaciones fueron relevantes en las

respuestas en las que se debían tener en cuenta las políticas y normativas de seguridad de la información. Así las cosas, esta guía se suma a otras iniciativas de colaboración interuniversitaria surgidas en la actual situación de crisis sanitaria.

La guía, que sigue el formato de preguntas y respuestas con el objeto de facilitar su consulta, se abre con unas recomendaciones que sintetizan las conclusiones de los cuatro apartados en los que se estructura en consonancia con las preocupaciones manifestadas por las universidades: (I) preguntas relacionadas con el ámbito de la docencia, (II) preguntas relacionadas con el ámbito de la evaluación, (III) preguntas relacionadas con el ámbito de la investigación y (IV) preguntas relacionadas con el tratamiento de datos de salud en el entorno laboral y en la gestión del teletrabajo (entendido éste en un sentido amplio y vinculado a las situaciones de movilidad creadas como consecuencia de la crisis actual), finalizando con unas breves conclusiones.

Por último, debemos señalar que las recomendaciones generales que se plantean en este documento constituyen únicamente la opinión conjunta de quienes han participado en su redacción. Corresponde a cada universidad, como responsable de los tratamientos de datos de carácter personal realizados en, y por, la institución, adoptar sus propias decisiones en función de las circunstancias de cada caso concreto contando con el asesoramiento de su DPD. **En consecuencia, según los arts. 38 y 39 RGPD, cada DPD podrá adoptar la interpretación que considere más adecuada según su propio criterio, entendiendo que las recomendaciones que contiene este documento carecen de eficacia vinculante.**

Abril de 2020

2. Recomendaciones

A modo de resumen ejecutivo, incluimos aquí un decálogo de recomendaciones generales básicas a cumplir respecto del tratamiento de datos personales por parte de las universidades en este periodo del COVID-19, en todos y cada uno de los ámbitos analizados en esta guía.

El Grupo de DPDs de la Sectorial de Secretarías Generales CRUE que ha participado en la elaboración del presente documento recomienda:

1. Insistir en que el derecho a la protección de datos es un derecho fundamental que no ha cedido por el estado de alarma. Desde esa perspectiva debe orientarse toda la información y gestión institucional en materia de protección de datos.
2. Recordar que no han sido derogadas ni suspendidas las normas universitarias, por lo que toda actuación universitaria debe siempre interpretarse en favor del mantenimiento de los derechos y obligaciones de la comunidad universitaria.
3. Tener en cuenta que la regulación de protección de datos permite adoptar medidas específicas frente a pandemias y necesidades de emergencia sanitaria en base a: protección de intereses vitales, interés público esencial, fines de medicina preventiva o laboral, diagnóstico médico, asistencia sanitaria o salud pública.
4. Cumplir con los principios y deberes en materia de protección de datos en docencia y evaluación virtual en las que se realizan tratamiento de datos. Lo mismo sucede para la investigación o para el trabajo en remoto. Todo ello sin olvidar la necesaria adaptación al estudiantado que tenga necesidades especiales. La declaración de estado de alarma no elimina los deberes en este terreno.
5. Informar, de manera ineludible, a alumnos y profesores sobre los tratamientos que se realizan en varias capas: guía docente, aula virtual e inicio de las pruebas conforme a modelos aprobados por cada universidad. Recordar la necesidad de que la información esté adaptada al estudiantado con diversidad funcional.
6. Realizar todos los tratamientos y uso de los datos personales bajo los principios de confidencialidad, menor uso de datos personales (minimización) y uso para las finalidades para las que fueron recogidos los datos, sin que puedan ser empleados para finalidades posteriores. Debe tenerse especial cuidado con el estudiantado con necesidades especiales.
7. Establecer recomendaciones internas en cada universidad dirigidas específicamente a cada colectivo de la comunidad universitaria sobre sus derechos y obligaciones.
8. Establecer, o recordar, la existencia de un canal específico para notificar incidencias en materia de protección de datos, así como mantener bien visibles los canales para el ejercicio de los derechos establecidos en el RGPD y en la LOPDGDD.
9. Emplear las herramientas oficiales que proporciona la universidad para pasar de un entorno presencial a un modelo de docencia, evaluación, investigación o trabajo en remoto u online. El empleo de cualquier otra herramienta, que no haya superado la necesaria evaluación de impacto en la privacidad de los miembros de la comunidad universitaria, puede poner en peligro la seguridad de la información, sin perder de vista el impacto en la imagen de la institución.

10. Resaltar el papel de los/las DPDs, o unidades o servicios de apoyo en materia de protección de datos de cada universidad, en primer lugar, como referencia en materia de consultas sobre dudas en protección de datos en el estado de alarma; y, en segundo lugar, como elementos indispensables de asesoramiento sobre las medidas o herramientas a implementar, y de concienciación para garantizar un correcto cumplimiento de la normativa y, en último término, el respeto de un derecho fundamental: el derecho fundamental a la protección de datos.

3. Índice de preguntas

4. Preguntas relacionadas con el ámbito de la docencia

La docencia o función educativa es una de las principales misiones que las normas atribuyen a las universidades. En el procedimiento docente se manejan un elevado número de datos personales, no sólo del alumnado, sino también del profesorado. La situación de emergencia y confinamiento generadas por la declaración del estado de alarma para hacer frente al coronavirus genera una serie de cuestiones relacionadas con la forma en la que tratar los datos personales en los procesos educativos en el entorno *online*.

Entre las preguntas frecuentes que surgen en este terreno podemos destacar las siguientes:

Pregunta 1: ¿Qué implicación tiene la normativa sobre protección de datos de carácter personal en la elección y el 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. La declaración de estado de alarma no exime de dicha obligación.

Deben utilizarse las herramientas oficiales provistas por cada institución y que dispongan de las garantías legales y de seguridad adecuadas. En el caso de contratarse servicios a proveedores externos que impliquen un tratamiento de datos de carácter personal, deberá elegirse únicamente un proveedor que ofrezca garantías suficientes y será necesaria la firma de un contrato de encargado del tratamiento que cumpla con los requisitos del art. 28 RGPD.

Pregunta 2: ¿Se pueden grabar las clases?

La declaración del estado de alarma imposibilita las clases presenciales. Por tanto, la necesidad de continuar la actividad docente obliga a realizarlas en modo no presencial. La grabación de una clase cumple con las siguientes funciones:

- Ofrecer la posibilidad de su visionado posterior en modelos de teleformación asíncrona.
- Garantizar la accesibilidad a los contenidos por parte de estudiantes que, por razones tecnológicas, personales o de salud, entre otras, no se hayan podido conectar.
- Constituir un material de estudio para la preparación de la evaluación.

Las grabaciones de imagen, sonido y texto pueden constituir un tratamiento de datos personales e incluyen contenidos protegidos por la propiedad intelectual. El principio de finalidad implica que las grabaciones únicamente deben ser utilizadas en el entorno de la asignatura, y profesorado y alumnado debe ser informados sobre el tratamiento de datos que se realiza. En el caso que un alumno o alumna quisiera grabar la clase por sus medios, debe contar con el consentimiento expreso de todos los asistentes.

Con carácter general, se recomienda emplear la grabación del 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.
- Favorecer las preguntas e interacciones sin activar la cámara.

Pregunta 3: ¿Cómo y de qué hay que informar cuando se graben las clases?

Deberá informarse acerca de las condiciones generales del tratamiento 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. Se recomienda que exista una capa de información si se usan metodologías que graben las clases.

Con carácter previo al inicio de la clase, antes de grabar, deberá advertirse al estudiantado que la sesión (imagen, sonido y chat) va a ser grabada de modo que éstos puedan desactivar su cámara/micrófono y en su caso participar a través del chat.

En particular debe advertirse al alumnado que debe preparar adecuadamente su espacio de interacción, de manera que se proteja la intimidad familiar y la de terceros. Las intervenciones en clase se consideran una parte más de la actividad docente, igual que en las clases presenciales. Asimismo, deberá advertirse del hecho de que las grabaciones no podrán ser usadas para otros fines.

Pregunta 4: ¿Se pueden difundir/publicar las clases grabadas?

Únicamente se deben utilizar los sistemas corporativos de la universidad. La descarga, difusión, distribución o divulgación de la grabación de las clases y particularmente su compartición en redes sociales o servicios dedicados a compartir apuntes atenta 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 prohibidos y podrían generar responsabilidad disciplinaria, administrativa y civil a la persona infractora. El profesorado puede reutilizar el material generado para otros fines académicos únicamente cuando aparezca su imagen y su voz, no la de estudiantes o terceras personas.

Pregunta 5: ¿Se puede ejercer el derecho de oposición a ser grabado en el desarrollo de una clase *online*?

Se podrá ejercer el derecho de oposición cuando exista una justificación adecuada (un familiar ha aparecido en segundo plano, grabación de imágenes no relacionadas con la docencia, diversidad funcional…) por parte del interesado que deba prevalecer sobre los intereses de la institución a tratar sus datos personales. La solicitud se resolverá por el órgano competente en la universidad según el procedimiento establecido al efecto.

La universidad debería articular para tales casos un procedimiento que también facilite el ejercicio de tal derecho, con carácter previo y antelación suficiente, así como la búsqueda en su caso de soluciones alternativas.

Pregunta 6: ¿Durante cuánto tiempo deben conservarse las clases grabadas *online*?

Con carácter general las grabaciones estarán disponibles como máximo durante el correspondiente curso académico, salvo que las mismas formen parte de las evidencias de evaluación del alumnado. No obstante, se podrá conservar una copia debidamente bloqueada para el cumplimiento de obligaciones legales por parte de la universidad. En el caso de que un profesor quisiera reutilizar estos materiales para otras actividades académicas deberá eliminar previamente cualquier dato personal de estudiantes o terceras personas.

En principio 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.

Pregunta 7: ¿Se pueden utilizar datos biométricos para controlar la asistencia y participación del alumnado en actividades *online*?

En principio, para controlar la asistencia y participación del alumnado se considera suficiente la utilización de los sistemas de identificación y acceso ordinarios del aula virtual que no impliquen el uso de datos biométricos.

Pregunta 8: ¿Cómo afecta al derecho a la protección de datos personales que la universidad solicite al estudiante que utilice sus propios dispositivos (ordenador, *tablet*, móvil…) para el seguimiento de la docencia *online*? ¿Y a que instalen en ellos un determinado programa o aplicación?

La conexión remota del estudiantado implica un tratamiento de datos de carácter personal. La universidad debe informar de las condiciones del mismo. En el caso de que para el seguimiento de las clases se empleen dispositivos compartidos, a fin de preservar la intimidad de terceros, se recomienda crear perfiles que preserven la privacidad del resto de personas que los utilicen.

Únicamente se puede requerir al alumnado que se instale en sus ordenadores aplicaciones para las que la universidad disponga de licencia y que garanticen la protección de los datos de carácter personal.

5. Preguntas relacionadas con el ámbito de la evaluación

Uno de los aspectos más delicados y controvertidos en el proceso educativo del alumnado se produce en la fase de evaluación de los conocimientos en tanto que la propia LOU, así como el Estatuto del Estudiante Universitario, la configuran como un derecho-deber. La LOU faculta a la institución universitaria para la verificación de los conocimientos.

Todo proceso de evaluación debe estar dotado de las correspondientes garantías. En este sentido, en esta especial situación que ahora acontece del coronavirus, debemos dotar de seguridad jurídica a los tratamientos vinculados a las nuevas modalidades de evaluación mediante las oportunas reformas normativas en los reglamentos de evaluación y/o revisión de exámenes de las universidades, así como en las correspondientes guías o programas docentes.

Entre las preguntas frecuentes que surgen en este terreno podemos destacar las siguientes:

Pregunta 9: ¿Se pueden grabar las pruebas de evaluación *online*?

Garantizar la seguridad a la hora de realizar una prueba de evaluación *online* se puede conseguir mediante su visionado, a través de canales de videoconferencia o mediante webcams, o bien, se puede proceder a la grabación de dicho visionado, que puede servir como evidencia de la evaluación. Piénsese, por ejemplo, en una prueba de evaluación oral.

Así las cosas, sí se pueden grabar las pruebas de evaluación. No obstante, la grabación efectuada deberá tener como finalidad garantizar la presencialidad del alumnado y la realización de la prueba, respetando en todo caso, y de manera inexcusable, el principio de proporcionalidad y la garantía de la dignidad y los derechos del estudiantado.

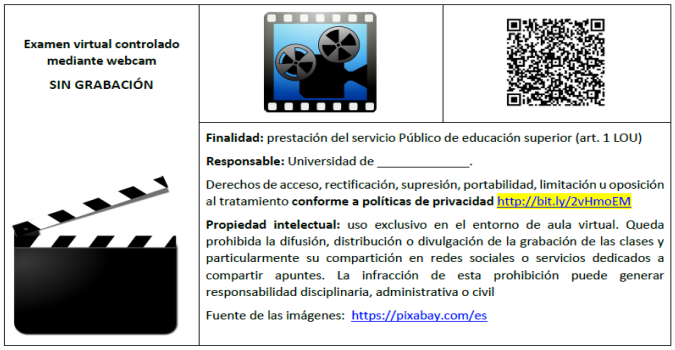
Asimismo, como todo tratamiento de datos implicará cumplir con unos objetivos básicos de transparencia, habrá que proceder a informar al alumnado (arts. 5.1.a) y 12 a 14 RGPD, y art. 11 LOPDGDD). En este ámbito la transparencia resulta imprescindible. En este sentido se ha señalado ya con anterioridad la necesidad de informar, al menos, en tres capas:

- Guía docente.
- Sistemas de notificación en el aula virtual.
- Al inicio de la prueba.

Esta estrategia puede completarse mediante el uso de:

- Envíos de circulares al profesorado y al estudiantado.
- Políticas de privacidad en el *website* de la universidad y/o en el aula virtual.
- Uso de una imagen gráfica en la primera pantalla de las transparencias que eventualmente se empleen.

Información gráfica para grabación



Información gráfica para control remoto

Pregunta 10: ¿El uso de una webcam puede afectar a la esfera de vida privada y familiar del alumnado y compañeras y compañeros en el aula? ¿Cómo y de qué debemos informar a la hora de grabar una prueba de evaluación *online*?

La captación de imágenes durante la realización de una prueba de evaluación virtual puede, siquiera, incidentalmente, afectar a la vida privada y familiar. Por ello, teniendo en cuenta la necesaria adaptación por diversidad funcional, es conveniente informar sobre:

- La naturaleza de la captación de imágenes definiendo de modo preciso el campo de acción de la webcam. En particular, en aquellos casos en los que la orientación de la misma implique la obtención de imágenes que abarquen parte de la estancia en la que el estudiantado desarrolla la actividad.
- La necesidad de informar a las personas que conviven con el o la estudiante de tales circunstancias, y recomendar su no acceso al entorno durante la realización de la prueba.
- La prohibición de captar imágenes de terceros, ya sea del profesorado, ya sea de otros compañeros o compañeras durante el proceso de evaluación, sin la correspondiente autorización.
- La exención de responsabilidad de la universidad en caso de no seguirse las recomendaciones.
- Las eventuales consecuencias académicas, si las hubiera, de no seguir estas recomendaciones.
- Aquellos extremos que la normativa de protección de datos exige a la universidad respecto de los tratamientos de datos personales que realice (arts. 13 y 14 RGPD y art. 11 LOPDGDD).

Es fundamental tener en cuenta la necesidad de eventuales adaptaciones cuando concurran circunstancias de diversidad funcional. En tal caso se recomienda informar al alumnado y adecuar si fuera necesario la prueba.

Pregunta 11: ¿Cómo se puede identificar al alumnado? ¿Se pueden usar datos biométricos o imágenes? ¿Qué métodos de identificación del alumnado se pueden emplear?

El Estatuto del Estudiante Universitario permite al profesorado solicitar la identificación del alumnado, quien deberá exhibir su carnet de estudiante o documento identificativo (art. 25.7). En un entorno *online*, se puede solicitar igualmente al alumnado que se identifique mostrando dicha documentación.

En todo caso, para la identificación del estudiantado se recomienda utilizar las medidas técnicas de las que ya dispone la propia universidad y que supongan la medida menos intrusiva para su privacidad.

Utilizar mecanismos de reconocimiento que empleen datos biométricos, más allá del uso de la imagen personal, requiere no sólo de la necesaria base legítima, sino de un análisis documentado de los riesgos vinculados al tratamiento de imágenes del que deriven la adopción de garantías específicas sin olvidar, para el caso de estar contratando dichos servicios a un tercero, la necesaria firma del correspondiente acuerdo o compromiso entre la universidad responsable y el tercero encargado (art. 28 RGPD y art. 33 LOPDGDD).

El Grupo de trabajo de la CRUE integrado por DPDs de las universidades españolas considera no recomendable las técnicas de reconocimiento facial. Debido a su complejidad técnica y al alto grado de exigencia que la legislación plantea al uso de datos biométricos, no es posible abordar esta cuestión sino desde la técnica de una evaluación de impacto relativa a la protección de datos. Por otra parte, la indefinición de las normas obliga a un proceso de interpretación de las habilitaciones para su uso que hace recomendable: Obtener un pronunciamiento expreso de las autoridades de protección de datos con competencia en la materia o definir junto con ellas el modelo de cumplimiento; y considerar las condiciones de regulación que ofrezcan una adecuada seguridad jurídica.

Pregunta 12: ¿Quién debe gestionar, conocer y tener acceso a los datos de estudiantes con necesidades especiales para su evaluación?

Tanto la LOU como el Estatuto del Estudiante Universitario y la Ley General de derechos de las personas con discapacidad y de su inclusión social (RDLeg. 1/2013) garantizan que el proceso formativo y de evaluación de los estudiantes con diversidad funcional se adapte a sus necesidades, lo que implicará adaptaciones metodológicas, temporales y espaciales. Serán las universidades las que determinen los casos del alumnado con necesidades especiales para su evaluación.

Las universidades cuentan con procedimientos específicos que aseguran el conocimiento y tratamiento de esta información personal por parte de las unidades o servicios con competencia para ello. Por otra parte, en cada universidad existen procedimientos de notificación a aquellos sujetos, incluidos en su caso el profesorado, que deben conocer de tales circunstancias para lograr los objetivos de igualdad y preservar la privacidad de los sujetos afectados.

No obstante, este conocimiento deberá estar presidido por los principios de minimización y finalidad en el tratamiento de datos personales (art. 5 RGPD), esto es, limitado a la

información necesaria para atender las necesidades existentes y por parte, exclusivamente, de quienes deban prestar asistencia o facilitar las medidas que se decidan, sin que dicha información pueda ser compartida o comunicada a quienes no tengan competencia al respecto. En este sentido, el profesorado sólo podrá conocer y tratar los datos estrictamente necesarios para el desarrollo de su tarea. Asimismo, sería recomendable recordar, de modo muy preciso, los deberes en materia de seguridad y confidencialidad.

Pregunta 13: ¿Se puede negar u oponerse un estudiante a ser grabado durante el desarrollo de una prueba de evaluación? ¿Cómo se debe actuar en esta situación? ¿Qué consecuencias tiene para el alumnado?

En un proceso de evaluación tanto estudiantado como profesorado son titulares de las facultades que integran el contenido esencial del derecho fundamental a la protección de datos, esto es: información o transparencia, acceso, rectificación, supresión, oposición, portabilidad y limitación del tratamiento (arts. 12 a 23 RGPD y arts. 11 a 18 LOPDGDD).

Con carácter general, la base de legitimación para el tratamiento invocada en el marco de un proceso de evaluación no es el consentimiento. Por ello, sin desconocer que las personas interesadas siempre podrán invocar sus derechos, debe tenerse en cuenta que:

- La oposición al tratamiento o la supresión de datos personales relacionados con aquellos extremos que configuren la prueba sujeta a evaluación usualmente resultará denegada prevaleciendo el deber de conservación de la misma.
- No obstante lo anterior, deberían considerarse los supuestos de oposición al tratamiento, por ejemplo, cuando deriven de circunstancias relacionadas con la diversidad, funcional, o la violencia de género.
- Se recomienda por ello, que la información previa a la realización del examen disponga de un cauce o procedimiento formal que permita a la institución universitaria conocer tales supuestos con la debida antelación.

La negativa de un o una estudiante a ser grabado, siempre y cuando no existan causas debidamente justificadas, y no existan otros medios que permitan identificarle y acreditar la realización de su prueba de evaluación, tendrán la repercusión académica que determinen las universidades. Es importante que este extremo sea comunicado al alumnado.

Pregunta 14: ¿Se puede negar el profesorado a ser grabado durante el desarrollo de una prueba de evaluación? ¿Cómo se debe actuar en esta situación? ¿Qué consecuencias tiene para el profesorado?

Tal y como ha quedado señalado, el profesorado, al igual que el estudiantado, son titulares de los derechos que el RGPD y la LOPDGDD les atribuyen (arts. 12 a 23 RGPD y arts. 11 a 18 LOPDGDD): información o transparencia, acceso, rectificación, supresión, oposición, portabilidad, limitación del tratamiento.

Con carácter general, la base de legitimación para el tratamiento de datos personales del personal de las universidades, públicas o privadas, ya sean personal funcionario o laboral, no obedece a la regla del consentimiento, sino que se sustenta sobre la base de su nombramiento público o de su contratación. Y en el caso de la grabación de una prueba de evaluación, el tratamiento de sus datos obedece a una utilización instrumental de su figura en el ejercicio de los derechos del alumnado a ser evaluado con objetividad y por seguridad jurídica del proceso administrativo llevado a cabo.

Así las cosas, en un proceso de evaluación, cuando la normativa universitaria o académica reconozca el derecho o el deber de grabación por motivos de seguridad jurídica de la prueba realizada, el profesorado no podrá oponerse a la misma.

Pregunta 15: ¿Puede un estudiante solicitar acceder a sus imágenes o pedir que se rectifiquen o cancelen?

Como parte de las facultades que integran el derecho a la protección de datos personales tratamiento (arts. 12 a 23 RGPD y arts. 11 a 18 LOPDGDD), el alumnado podrá solicitar el acceso a sus imágenes, siempre que las mismas hayan sido grabadas, 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, lo que también vendrá determinado en la citada normativa académica.

En relación con la posibilidad del estudiantado de solicitar la rectificación de sus imágenes en las pruebas de evaluación, por su propia naturaleza la conservación de una prueba de evaluación únicamente admitiría la rectificación en casos como los relativos a la identificación de las personas concernidas.

Por último, en relación con la posibilidad de solicitar la cancelación o supresión de datos personales relacionados con aquellos casos en los que la grabación sirva como evidencia de la evaluación, como regla general, resultará denegada dicha petición prevaleciendo el deber de conservación de la misma tal y como se disponga en la normativa académica correspondiente.

Pregunta 16: ¿Durante cuánto tiempo deben conservarse 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 de las pruebas de evaluación que establezcan cada una de las universidades.

El Estatuto del Estudiante Universitario indica (art. 29.3) 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 autonómica 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.

Así pues, la grabación de aquellas pruebas y evidencias de evaluación se deberá conservar durante el tiempo que prevean cada una de las universidades para estos supuestos.

Se recuerda en este punto que la conservación de las pruebas 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.

Pregunta 17: ¿Cómo se deben publicar las calificaciones durante la evaluación *online*?

La publicación de las calificaciones en un proceso de evaluación *online* sigue las mismas reglas que su publicación durante un proceso de evaluación presencial: deberán ser publicadas en los espacios virtuales habilitados a tal fin y a los que sólo pueda acceder el alumnado implicado en el proceso de evaluación, nunca en espacios abiertos a los buscadores.

La forma en la que proceder a publicar las calificaciones -hecho habilitado por la LOU- debe, en primer lugar, estar limitada a los datos mínimos necesarios para que el estudiantado pueda identificarse (art. 5.1.c) RGPD); y, en segundo lugar, seguir las Orientaciones de la AEPD sobre publicación de los documentos de identificación personal (disp. adic. 7ª LOPDGDD). Así:

- Se desaconseja la publicación mediante el uso de documentos adjuntados en el aula como documentos PDF, siendo lo recomendable el uso de módulos de gestión de calificaciones de la propia plataforma institucional.
- Las calificaciones se publicarán principalmente con nombre y apellidos de los y las estudiantes y la calificación obtenida.
- En el caso de que pueda darse la situación de que en un mismo grupo dos estudiantes coincidan en nombre y apellidos, podrá utilizarse también el DNI.
- Si se procede a utilizar el DNI, el mismo nunca aparecerá de forma completa, sino que deberá aparecer de forma ofuscada siguiendo las Orientaciones de la AEPD al respecto (https://www.aepd.es/sites/default/files/2019-09/orientaciones-da7.pdf).

Por otro lado, atendiendo al principio de finalidad del tratamiento, debemos recordar que:

- La publicación de las calificaciones en las aulas virtuales o espacios habilitados para ello, únicamente se mantendrá accesible durante el periodo previsto en la normativa académica, garantizando su conocimiento por los interesados, así como el ejercicio de los derechos de revisión y, en su caso, posterior reclamación.
- Resulta conveniente informar al estudiantado de la finalidad de la publicación y la prohibición expresa de hacer uso para fines diferentes y, en particular, respecto de las calificaciones de otras personas.

Pregunta 18: ¿Cómo se deben hacer las revisiones de las pruebas de evaluación *online*? ¿Se pueden mandar por correo electrónico las evidencias de la evaluación?

La revisión, ante la situación de no presencialidad fruto de la situación provocada por el coronavirus, deberá seguir una modalidad *online*.

Atendiendo a los principios de transparencia y seguridad jurídica, se debe informar de forma clara y precisa de plazos y modo de revisión por parte del profesorado, siguiendo en todo caso la regla general y plazos de revisión previstos en la normativa académica y universitaria.

Para las revisiones se utilizarán los medios establecidos por la universidad. Si bien, usualmente se producirán las revisiones de forma asíncrona con la presentación de alegaciones por el alumnado y por anotaciones del profesorado a través de la correspondiente aula virtual, de trasladarse el modelo de revisión presencial a un entorno *online* podrían, asimismo, emplearse métodos de videoconferencia.

El grupo de trabajo de DPDs de la CRUE desaconseja el uso del correo electrónico no sólo por la posible afectación a las expectativas de privacidad de los usuarios, sino porque, además, las cuentas de correo electrónico son más vulnerables en términos de seguridad, permiten descargas no recomendables, e incluso borrados accidentales que podrían afectar al

mantenimiento de evidencias imprescindibles para salvaguardar los derechos de las personas evaluadas.

Asimismo, debemos recordar que de la misma manera que los procedimientos de evaluación debían ser adaptados a las necesidades específicas de los estudiantes con diversidad funcional, también lo deben ser los procedimientos de revisión.

Pregunta 19: ¿Qué procedimiento se debe seguir ante una incidencia en el proceso de evaluación?

Durante un proceso de evaluación *online* nos podremos encontrar no sólo con las incidencias propias y comunes a las pruebas presenciales, sino con incidencias de tipo técnico.

La detección de actos fraudulentos se someterá a los procedimientos de disciplina universitaria previstos académicamente, y siguiendo lo establecido en el Reglamento de Disciplina Académica (Decreto de 8 de septiembre de 1954). El tratamiento de la información necesaria para el citado proceso deberá seguir los cauces previstos en la normativa universitaria y académica y ser comunicada única y exclusivamente a los órganos competentes con la citada finalidad.

Ante las incidencias por cuestiones técnicas o sobrevenidas no imputables a ninguno de los sujetos que intervienen -entre las que se deberán valorar las derivadas de los efectos de ser víctima, directa o indirecta, del coronavirus-, se deberá habilitar un día y horas diferentes para su realización. Esto implicará, en la actual situación, tener en cuenta no sólo lo previsto en la normativa académica, sino la disponibilidad y el soporte técnico necesario y existente.

Se recuerda en este punto la necesidad de contar con un canal de comunicación de incidencias que sea conocido por profesorado y alumnado, y con servicios que hagan viable la portabilidad de la información del proceso de evaluación, así como su durabilidad y accesibilidad a las necesarias evidencias de realización de la prueba de evaluación y de las incidencias ocurridas.

6. Preguntas relacionadas con el ámbito de la investigación

Las universidades son centros de generación y transferencia del conocimiento que, entre sus funciones, se dedican a la investigación. En este sentido, la aparición del coronavirus ha generado toda una serie de proyectos de investigación que implican, en muchos casos, el manejo de un elevado número de datos personales, que en muchos casos son datos relacionados con la salud del sujeto.

Entre las preguntas frecuentes que surgen en este terreno podemos destacar las siguientes:

Pregunta 20: ¿Pueden eliminarse algunos de los requisitos que se venían exigiendo en materia de protección de datos a los proyectos de investigación, debido a la urgencia de la situación?

No. Las investigaciones sobre el COVID-19, sean o no urgentes, están sometidas a las previsiones ya establecidas sobre investigación y protección de datos. En este sentido téngase en cuenta que la normativa de protección de datos nos ofrece las herramientas necesarias para proteger este derecho fundamental y adaptarse a una situación como la actual (Informe AEPD N/REF: 0017/2020).

El tratamiento de datos con fines de investigación científica estará sujeto a las garantías adecuadas para los derechos y las libertades de los interesados. De este modo se dispondrá de las medidas técnicas y organizativas pertinentes para ese cometido, con especial atención al respeto del principio de minimización, es decir, emplear sólo los datos adecuados y pertinentes con relación al fin perseguido (arts. 5 y 89 RGPD).

En este sentido, conviene destacar que investigaciones con datos de salud, y otras muchas con datos sensibles, de colectivos vulnerables, de víctimas de violencia de género, con datos genéticos, biométricos, etc., requieren, aparte de su "registro de actividades de tratamiento", de un "informe de evaluación de impacto" elaborado con la ayuda y asesoramiento del DPD (ver la lista completa de tratamientos de datos personales que requieren informe de evaluación de impacto en https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf).

Pregunta 21: ¿Es necesario que los DPDs revisen las investigaciones sobre el COVID-19?

Depende del objeto de la investigación. Obviamente las investigaciones en plantas o animales no requieren de la presencia del DPD, pero si la investigación necesita utilizar y tratar datos personales debe contar con su asesoramiento.

En este sentido hay que recordar la existencia de Comités de ética, especialmente en la investigación biomédica, que tienen que emitir informes previos. En dichos Comités debe estar integrado el DPD o, en su defecto, un experto con conocimientos suficientes en el RGPD (disp. adic. 17ª.2.g) LOPDGDD). Estos Comités deberían participar en toda investigación con datos personales, dado que la Unión Europea entiende que la "ética de los datos" alcanza a aquellas investigaciones con personas físicas en la que se tratan datos personales, y cumplir con los distintos aspectos que conforman el derecho de protección de datos de carácter personal es un requerimiento ético en sí mismo, al margen de las consideraciones jurídicas.

En el caso de que la universidad no hubiera incluido en el Comité de ética al DPD, también es necesario la supervisión del proyecto de investigación por parte de éste cuando dicho proyecto requiera el tratamiento de datos personales. En efecto, la normativa prevé que responsables y encargados de tratamiento garanticen que el DPD participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales (arts. 38 y 39 RGPD).

Pregunta 22: Si en el proyecto del COVID-19 participan varias entidades, ¿cómo gestionamos el cumplimiento de la normativa de protección de datos? ¿hay que firmar convenios?

Es necesario realizar un análisis previo de la situación y de las funciones que tenga cada socio para determinar cómo procede actuar. Conviene que este análisis sea supervisado por el DPD.

En principio, cabrían dos situaciones teóricas:

- por un lado, si hay una entidad líder, entonces ella será la responsable del tratamiento de datos personales y el resto tendrán que firmar un contrato de encargado de tratamiento (en la medida en que tratan datos por cuenta de aquel responsable);
- por otro lado, si no existe tal líder único ya que las entidades determinan conjuntamente los objetivos y los medios del tratamiento de datos, en ese supuesto todas ellas serán corresponsables de tratamiento y tendrán que firmar un acuerdo de esa naturaleza.

Como se ve, en ambos casos hay que firmar un acuerdo entre las partes (arts. 26 y 28 RGPD, y 28 y 29 LOPDGDD). Ese instrumento jurídico establecerá la relación entre los socios y fijará las cláusulas que definan las obligaciones respectivas en materia de protección de datos (https://www.aepd.es/media/guias/guia-directrices-contratos.pdf).

Si se producen transferencias de datos a terceros países, o sea, fuera de la Unión Europea, tienen que existir garantías adecuadas (arts. 46 RGPD y 41 y 42 LOPDGDD), aunque lo conveniente es consultar con el DPD ya que puede haber distintas opciones que incluyen casos excepcionales.

Pregunta 23: ¿Cómo informo a los miembros de mi comunidad universitaria sobre un proyecto del COVID-19 por si les interesa participar en él?

La opción más sencilla es subir el correspondiente anuncio en la web de la universidad incorporando un contacto al efecto. También es posible que ya exista una zona de comunicación de proyectos en esa web.

Otra opción válida puede ser emplear una lista de distribución, siempre que presente garantías y la propia universidad la supervise. La gestión de ese directorio tiene que estar dada de alta en el registro de actividades de tratamiento de la universidad. Por lo general, habrá que contactar con los responsables de comunicación de la universidad para que validen la solicitud.

Al margen de esas cuestiones, también es efectivo diseñar un pdf, documento electrónico o enlace para su difusión a través de los canales institucionales corporativos en redes sociales.

Pregunta 24: ¿Y qué pasa con la investigación en salud?

Habida cuenta de su relevancia, la investigación en salud tiene previsiones específicas, que esquemáticamente son las siguientes:

- Aunque se pueda solicitar el consentimiento para los proyectos de investigación, en situaciones de excepcional relevancia y gravedad las autoridades sanitarias pueden llevar a cabo estudios científicos sin ese consentimiento de los afectados.
- El Comité Europeo de Protección de Datos, sin embargo, considera más apropiadas que el consentimiento, las bases de interés público (cuando el ensayo sea resultado de una tarea encomendada a un organismo público o privado por una ley nacional) o de interés legítimo (disposición adicional 17.2.d) LOPDGDD).
- En el caso de ensayos clínicos desarrollados con base en el consentimiento son válidos, pero se aconseja revisar la información suministrada en su momento, para en su caso, complementarla, de acuerdo con los arts. 13 y 14 RGPD.
- El RGPD permite tanto el tratamiento como la cesión de datos sin consentimiento cuando sea necesario para "proteger intereses vitales del interesado o de otra persona física" (considerandos 46 y 112 RGPD y arts. 9.1.c) y 49.1.f) RGPD).
- Se permite reutilizar los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial (con la autorización del Comité de ética). Sin embargo, en ensayos clínicos se exige un consentimiento específico (aunque puede no ser imprescindible este último pues el art. 5.1.b) RGPD permite el tratamiento ulterior de los datos con fines de investigación siempre que se cumplan las salvaguardas establecidas en el art. 89 RGPD).
- Se pueden excepcionar determinados derechos de protección de datos (acceso, rectificación, limitación y oposición) en ciertas circunstancias (disp. adic. 17ª.2.e) LOPDGDD);
- Es lícito el uso de datos personales seudonimizados, siempre que haya una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización, y que en el equipo de investigación exista un compromiso expreso de confidencialidad y se adopten medidas de seguridad específicas (con la autorización del Comité de ética).

Cuando se tratan datos con fines de investigación en salud pública, además de lo dicho, habrá que realizar una evaluación de impacto para determinar los riesgos, someter esa investigación a las normas de calidad, adoptar medidas para que los investigadores no accedan a datos de identificación de los interesados, y, en el caso de promotores de ensayos clínicos no europeos, designar un representante legal establecido en la Unión Europea (arts. 9 y 89 RGPD; disp. adic. 17ª LOPDGDD).

Pregunta 25: ¿Cómo seudonimizo los datos de mi investigación?

Por seudonimización hay que entender el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a impedir esa reversión.

Existen diversas técnicas para seudonimizar datos, por lo que lo más recomendable es consultar al responsable de seguridad o al responsable de información de la universidad, o, en su defecto, a los servicios informáticos. También puede consultarse el estudio de la AEPD

sobre la técnica Hash https://www.aepd.es/sites/default/files/2019-11/estudio-hash-anonimidad.pdf

Hay que tener presente que la reversión no autorizada de la seudonimización es un riesgo para los derechos y libertades de las personas físicas, por lo que el responsable y el encargado de tratamiento deben adoptar las medidas adecuadas, técnicas y organizativas, para que no suceda tal violación de seguridad de los datos (considerandos 26, 28, 29, 75, 85 y 156 RGPD y arts. 4.5, 6.4.e), 25.1, 32.1.a), 40.2.d) y 89.1 RGPD; y 28.2.a) y disp. adic. 17ª LOPDGDD).

En los fines de investigación científica lo más recomendable es acudir a la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Si los fines se pueden alcanzar mediante un tratamiento ulterior que no permita la identificación de los interesados, entonces la seudonimización se vuelve obligatoria. En investigación en salud hay previsiones específicas (nos remitimos a la pregunta anterior).

Pregunta 26: ¿Qué se debe hacer cuando no es posible obtener el consentimiento del interesado y los datos personales no se pueden disociar?

Como regla especial, la LOPDGDD permite a las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública (disp. adic. 17ª.2.b) LOPDGDD).

Al margen de lo expuesto, y salvo causa muy justificada, como es la protección de intereses vitales de las personas, el acceso a datos de historias clínicas solo está legalmente previsto, al margen de las investigaciones judiciales, para las autoridades de la sanidad pública, "por razones epidemiológicas o de protección de la salud pública" y con una serie de garantías y justificaciones, por lo que solo podría realizarse a través de ellas y con su pertinente autorización, en la forma prevista en la legislación sobre derechos del paciente (art. 16 Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica).

Pregunta 27: ¿Debo presentar mi proyecto al Comité de ética o bioética?

La regulación de estos Comités es diversa teniendo en cuenta la distinta normativa sectorial. También la situación en las universidades no es homogénea en este tema.

En la normativa sobre investigación biomédica esta obligación es evidente al preverse la existencia de Comités de ética de la investigación. Dichos Comités tienen como misión garantizar el respeto a la dignidad, integridad e identidad del ser humano en lo que se refiere a la investigación con humanos, con muestras biológicas o con datos de origen humano, así como promover un comportamiento ético en la investigación. Por tanto, entre sus competencias está el velar por el cumplimiento de la normativa vigente aplicable en materia de protección de datos y de investigación.

De hecho, la propia LOPDGDD obliga a que los Comités de ética en el ámbito de la salud, biomédico o del medicamento, integren al DPD o, en su defecto, un experto con los conocimientos previstos en el RGPD (disposición adicional 17ª.2.h) LOPDGDD; Ley 14/2007, de 3 de julio, de Investigación biomédica).

Pregunta 28: ¿Hay que tener presente el Esquema Nacional de Seguridad (ENS)?

El ENS es, básicamente, un conjunto de medidas de seguridad de obligatorio cumplimiento para las universidades públicas. Las universidades privadas no están sujetas al mismo, pero pueden adherirse. El objetivo del ENS es fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas (Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica).

En cualquier caso, resulta fundamental que, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del proyecto de investigación aplique las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo detectado, medidas que, en el ámbito de las universidades públicas, deberán ser conformes con las que contiene el ENS (disp. adic. 1ª LOPDGDD).

Asimismo, en materia de seguridad, todo investigador debe saber que más importante que las medidas generales de seguridad, son las medidas de seguridad individuales y específicas que se deben adoptar por parte de todos los investigadores para proteger los datos personales.

7. Preguntas relacionadas con el tratamiento de los datos de salud en el entorno laboral y en la gestión del teletrabajo

Las universidades, públicas y privadas, están enfrentándose a tratamientos no previstos de datos personales (incluyendo datos de categorías especiales, como los de salud) tanto de sus empleados como de otros miembros o personas vinculadas a la comunidad universitaria, o de sus familiares. En particular, en la gestión de planes especiales de contingencia en el ámbito de la prevención de riesgos laborales, así como en la implantación urgente del teletrabajo.

Trabajar en remoto en tiempos del COVID-19 implica proteger la salud de todos, proteger los datos personales y proteger la intimidad y el derecho a la desconexión digital. Las cuestiones que pueden surgir se alinean en los escenarios descritos.

El RGPD y la LOPDGDD, en conjunción con otras normas sectoriales (estatales o autonómicas) y, particularmente, las que se están adoptando en el contexto de la declaración del Estado de Alarma para hacer frente de forma inmediata y eficaz a esta coyuntura, contienen las reglas necesarias para permitir legítimamente dichos tratamientos. Este conjunto de normas nos debe permitir afrontar estos nuevos tratamientos de plena conformidad con la normativa de protección de datos personales.

Entre las preguntas frecuentes que se plantean en este terreno podemos destacar las siguientes:

7.1. Protección de los datos de salud en el entorno laboral

Pregunta 29: ¿Puede la universidad tratar la información de si sus trabajadores están infectados del coronavirus? ¿Puede la universidad tratar de detectar a las personas infectadas integrantes de su comunidad?

El dato de salud es un dato de categoría especial por lo que su tratamiento además de una de las bases de legitimación contenidas en el art. 6 RGPD requiere que se dé alguna de las circunstancias del art. 9.2 RGPD entre los que a los presentes efectos interesan las contenidas en sus letras b), c), h) e i).

En este sentido, cabe concluir que la cláusula de interés vital se proyecta no sólo sobre la persona interesada sino también otras personas físicas, entre las que obviamente cabe incluir el entorno de trabajo y la comunidad universitaria

Igualmente la Ley de Prevención de Riesgos Laborales impone, por un lado, la obligación del empleado de comunicar cualquier situación que, a su juicio, entrañe, por motivos razonables, un riesgo para la seguridad y la salud de los trabajadores; y por otro la obligación del empleador de proteger la salud de sus empleados, pudiendo realizarles los reconocimientos imprescindibles para verificar si el estado de salud del trabajador puede constituir un peligro para el mismo, para los demás trabajadores o para otras personas relacionadas con la empresa, previo informe de los representantes de los trabajadores y conforme a lo dispuesto en el art. 22 de Ley de Prevención de Riesgos Laborales.

Esa información también puede ser obtenida mediante preguntas al personal. Sin embargo, las preguntas deberían limitarse exclusivamente a indagar sobre la existencia de síntomas, o si la persona trabajadora ha sido diagnosticada como contagiada, o sujeta a cuarentena. Resultaría contrario al principio de minimización de datos la circulación de cuestionarios de salud extensos y detallados, o que incluyan preguntas no relacionadas con la enfermedad.

En consecuencia, deberían entenderse adecuados todos los tratamientos de datos personales que, de acuerdo con la legislación vigente y cumpliendo con las garantías adecuadas, vayan dirigidos a la detección precoz del coronavirus, incluidos aquellos controles médicos que se impongan desde el punto de vista del desarrollo de vigilancia obligatoria de la salud. Estas medidas, serán particularmente relevantes en casos de clínicas universitarias, centros que cuenten con profesionales con plaza vinculada expuestos al riesgo, o profesionales y/o estudiantes con riesgo de exposición al agente infeccioso.

Pregunta 30: ¿Pueden transmitir esa información al personal de la universidad?

La comunicación de datos personales, en su condición de tratamiento de datos personales, debe cumplir con los requisitos exigibles por el art. 6 RGPD y, en el presente supuesto, por el art. 9.2 RGPD.

Así se deberá ponderar necesariamente los intereses en juego, en especial el derecho de otras personas a la protección de su salud, debiendo respetarse especialmente el principio de minimización de datos, de modo que solo se transmita la información necesaria para alcanzar la finalidad, evitando en todo momento identificar o dar datos que permitan la identificación del personal afectado por la enfermedad y preferentemente en coordinación con los Servicios de Prevención.

Pregunta 31: ¿Se puede pedir a las personas trabajadoras y visitantes de la universidad datos sobre países que hayan visitado anteriormente, o si presentan sintomatología relacionada con el coronavirus?

La Ley de Prevención de Riesgos Laborales, en su art. 21, impone la obligación del empleador de proteger la salud de sus empleados, pudiendo realizar los reconocimientos imprescindibles para verificar si el estado de salud del trabajador puede constituir un peligro para el mismo, para los demás trabajadores o para otras personas relacionadas con la empresa, previo informe de los representantes de los trabajadores y conforme a lo dispuesto en el art. 22 Ley de Prevención de Riesgos Laborales.

Esa información también puede ser obtenida mediante preguntas al personal. Asimismo, con la finalidad preventiva de evitar la propagación del virus y por interés vital de la comunidad universitaria, se podrá consultar a los visitantes de la institución. Sin embargo, las preguntas deberían limitarse exclusivamente a indagar sobre la existencia de síntomas, o si la persona trabajadora ha sido diagnosticada como contagiada, o sujeta a cuarentena. Resultaría contrario al principio de minimización de datos la circulación de cuestionarios de salud extensos y detallados, o que incluyan preguntas no relacionadas con la enfermedad.

Pregunta 32: ¿Se pueden tratar los datos de salud de las personas trabajadoras relacionados con el coronavirus?

El dato de salud es un dato de categoría especial por lo que su tratamiento además de una de las bases de legitimación contenidas en el art. 6 RGPD requiere que se dé alguna de las

circunstancias del art. 9.2 RGPD entre los que a los presentes efectos interesan las contenidas en sus letras b), c), h) e i).

En este sentido, cabe concluir que la cláusula de interés vital se proyecta no sólo sobre la persona interesada sino también sobre otras personas físicas, entre las que obviamente cabe incluir el entorno de trabajo y la comunidad universitaria.

La obligación que la Ley de Prevención de Riesgos Laborales impone de velar por la seguridad y salud de sus empleados y de adoptar las medidas necesarias necesita del tratamiento de datos de salud, sin perjuicio de que por parte de los Servicios de Prevención correspondientes se realicen los seguimientos y comprobaciones que sean necesarios para asegurar dicha protección.

Pregunta 33: ¿En qué medida la universidad debe ceder datos de personal contagiado por el COVID-19 a las autoridades sanitarias? ¿qué otras cesiones de datos pueden plantearse en este escenario?

La cesión de datos personales en relación con la epidemia de COVID-19 debe encuadrarse en la colaboración con las autoridades sanitarias y se realizará atendiendo a los requerimientos que realicen las mismas.

En el caso de la cesión de datos de personal contagiado por el COVID-19, como señala la AEPD, los datos pueden, y debieran al ser una enfermedad de declaración obligatoria, transmitirse a las autoridades sanitarias competentes, preferiblemente a través de los Servicios de Prevención. La información debe proporcionarse respetando los principios de finalidad, proporcionalidad y siempre dentro de lo establecido en las recomendaciones o instrucciones emitidas por las autoridades competentes, en particular las sanitarias.

Adicionalmente, pueden darse otros supuestos en los que debieran suministrarse los datos del profesorado de las áreas de Ciencias de la Salud a requerimiento de la autoridad sanitaria competente, hay que tener en cuenta que son datos profesionales y que la mayoría de las universidades cuentan con un directorio de sus profesionales.

En relación con el suministro de datos de estudiantes en el último curso de Medicina o Enfermería por parte de las universidades a las autoridades sanitarias competentes, se deberá considerar la aplicación de los distintos principios e intereses en juego.

La base de legitimación en estos casos, al no incluir información sobre datos de salud, podría encontrarse en la letra c) o en la letra e) del art. 6 RGPD.

También puede plantearse un supuesto de cesión a la inversa, cuando la administración sanitaria o un tercero comunica a las universidades casos de contagio confirmados de personas empleadas suyas. Cuando un tercero (sea una autoridad sanitaria, un familiar u otro trabajador, por ejemplo) proporcione a la universidad información sobre la salud de uno de sus empleados, la universidad actuará conforme a los protocolos que tenga establecidos para el cumplimiento de obligaciones legales en el ámbito laboral y en especial lo relativo a sus obligaciones en el ámbito de la prevención de riesgos laborales, canalizando dicha información a través de los Servicios de Prevención.

Pregunta 34: En caso de cuarentena preventiva o estar afectado por el coronavirus ¿la persona trabajadora tiene obligación de informar a su empleador de esta circunstancia?

La Ley de Prevención de Riesgos Laborales impone la obligación al trabajador de Informar de inmediato a su superior jerárquico directo, y a los trabajadores designados para realizar actividades de protección y de prevención o, en su caso, al servicio de prevención, acerca de cualquier situación que, a su juicio, entrañe, por motivos razonables, un riesgo para la seguridad y la salud de los trabajadores.

Resulta evidente con la declaración del estado de alarma y las medidas adoptadas por las autoridades sanitarias que el hecho de estar afectado por coronavirus o en cuarentena preventiva entraña un riesgo para la salud de los trabajadores por lo que estos están obligados a comunicar dicha situación, preferentemente a través de los Servicios de Prevención.

Pregunta 35: ¿El personal de seguridad puede tomar la temperatura a los trabajadores con el fin de detectar casos de coronavirus?

El art. 21 Ley de Prevención de Riesgos Laborales establece la obligación para el empleador de informar del riesgo y de las medidas adoptadas. Entre esas medidas puede estar la toma de temperatura por parte del personal que controle el acceso. El tratamiento debe garantizar los principios recogidos en el RGPD. Considerando que el hecho de detectar síntomas febriles no supone necesariamente que se esté enfermo de COVID-19, la evaluación deberá realizarse a través de los Servicios de Prevención.

El seguimiento, en su caso, deberá realizarse conforme al art. 22.6 Ley de Prevención de Riesgos Laborales, de modo que "las medidas de vigilancia y control de la salud de los trabajadores se llevarán a cabo por personal sanitario con competencia técnica, formación y capacidad acreditada".

7.2. Protección de datos personales en la gestión del teletrabajo

Pregunta 36: En las actuales circunstancias ¿cuál es la base de legitimación para el teletrabajo, tanto para los eventuales tratamientos de datos, como para la adopción de la medida en sí misma?

Las circunstancias actuales y el Derecho aplicable, tanto al teletrabajo como a los tratamientos que pudieran derivar de esta nueva modalidad de prestación del servicio, se legitiman en base al art. 6.1.c) RGPD, cumplimiento una obligación legal aplicable a la universidad, como responsable de dichos tratamientos.

Así, observamos cómo el Real Decreto 463/2020, por el que se declara el estado de alarma, adoptó una serie de medidas en relación con la limitación de la movilidad de las personas, incluyendo desplazamientos al lugar de trabajo para efectuar la prestación laboral, profesional o empresaria, al objeto de contener el avance del COVID-19 (art. 7). En el ámbito educativo, suspendió la actividad educativa presencial en todos los centros y etapas, ciclos, grados, cursos y niveles de enseñanza incluida la enseñanza universitaria (art. 9.1) y, estableció que durante el periodo de suspensión se mantendrían las actividades educativas a través de las modalidades a distancia y *online*, siempre que resultase posible (art. 9.2).

Frente a la cesación temporal o reducción de la actividad, el Real Decreto-ley 8/2020, de 17 de marzo, de medidas urgentes extraordinarias para hacer frente al impacto económico y social del COVID-19 (art. 5), da carácter preferente a la modalidad de trabajo a distancia. Y esta previsión alcanza incluso a sectores, empresas o puestos de trabajo en las que no estuviera prevista dicha modalidad.

Pregunta 37: ¿Cómo debe procederse ante los nuevos riesgos para los derechos y libertades de las personas interesadas en un contexto de teletrabajo?

En un contexto de teletrabajo, la universidad viene obligada a evaluar los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas y aplicar medidas técnicas y organizativas apropiadas (art. 24 RGPD), que resultará particularmente relevante en materia de seguridad conforme al art. 32 RGPD.

Tanto el DPD, como el responsable del tratamiento y el responsable de seguridad de la información deben participar desde el inicio en el proceso de diseño institucional del modelo de teletrabajo que se adopte, dado que aplica el principio de seguridad proactiva desde el diseño y por defecto (art. 25 RGPD), con el fin de diseñar y aplicar las medidas técnicas u organizativas apropiadas (art. 5.2 RGPD).

Los riesgos para los derechos y libertades de las personas interesadas en un contexto de teletrabajo resultan esencialmente riesgos vinculados a la seguridad y, en este sentido, debe ser el responsable de seguridad, en las universidades públicas, quien, según el art. 10 del ENS, determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. Para ello tendrá particularmente en cuenta que las medidas a las que se refiere el art. 32 RGPD deben considerar las previsiones del ENS en los siguientes artículos: art. 16, sobre autorización y control de accesos; art. 22, en relación con otros sistemas de información interconectados; art. 23 sobre registros de actividad; así como las medidas del Anexo II en materia de acceso remoto.

En el caso de las universidades privadas, a pesar de no tener la obligación legal recogida en la LOPDGDD, es recomendable adaptar un conjunto de controles similar a los exigidos por el ENS.

Pregunta 38: ¿Se debe definir una política de protección de la información para situaciones de movilidad o teletrabajo?

La excepcional situación en la que nos encontramos ha abocado a la mayoría de las universidades a poner en marcha soluciones de teletrabajo provisionales, sin una previa planificación. Cuando la situación se prolonga, es aconsejable realizar una reflexión y adecuar la implementación del teletrabajo, mediante la definición de una política o normativa específica de protección de la información para situaciones de movilidad o teletrabajo (en el marco de la política general (o políticas) en materia de protección de datos y seguridad de la información), en cuya elaboración participen tanto el DPD, como el responsable del tratamiento y el responsable de seguridad de la información.

Es recomendable que dichas políticas o normativas sean planificadas entre DPDs y Responsables de seguridad de la información u órganos correspondientes, y reciban la adecuada difusión.

Pregunta 39: ¿Está obligado el personal a suministrar su número de teléfono privado?

El art. 5 Real Decreto-Ley 8/2020, de 17 de marzo, de medidas urgentes extraordinarias para hacer frente al impacto económico y social del COVID-19 establece el carácter preferente del trabajo a distancia.

Las universidades asignan a su personal direcciones de correo electrónico, incluso individualizadas, y cuentan con soluciones de VoIP, que permiten disponer del teléfono de la oficina en casa durante la jornada laboral.

Por tanto, la existencia de medios menos invasivos de los derechos fundamentales del personal para la comunicación con ellos conlleva una respuesta negativa a la petición del teléfono o correo electrónico personal, considerando suficientes los medios ya disponibles, que podrían abarcar el desvío de llamadas a petición del interesado.

Pregunta 40: ¿Pueden los empleados hacer uso de medios propios como vía de comunicación, con los interesados o entre ellos (*Skype*, *WhatsApp*, *Telegram* o equivalente)? ¿Se pueden crear grupos de *whatsapp* para teletrabajo?

Los empleados deben usar como vía de comunicación con los interesados las vías y medios establecidos por la universidad, ya sea mediante el uso de los correos institucionales que gestionen o de otras herramientas utilizadas para este fin.

En el caso de la comunicación entre los propios empleados podríamos encontrarnos en dos supuestos:

1. Estos medios se utilizan como forma de comunicación para teletrabajar.
2. Estos medios se utilizan como forma de comunicación entre compañeros de trabajo, pero para temas personales, no relacionados con su trabajo en la universidad, que entraría, en nuestra opinión, dentro de la excepción de actividades domésticas del art. 2.2.c) RGPD y no estaría sometido al mismo.

Cuando las plataformas de mensajería instantánea se usen como forma de comunicación para el teletrabajo, estaríamos ante un tratamiento de datos que deberá cumplir las exigencias del RGPD, en especial lo relativo al cumplimiento de los deberes de información y del principio de protección de datos desde el diseño y por defecto y a la formalización del oportuno contrato de encargado de tratamiento.

Deberán de preverse las formas de hacer efectivo el derecho a la desconexión digital recogido en el art. 88 LOPDPGDD, con el que se pretende garantizar el respeto al tiempo de descanso, permisos y vacaciones, así como la intimidad personal y familiar del empleado fuera del tiempo de trabajo establecido.

Pregunta 41: ¿Qué recomendaciones pueden darse a las personas empleadas para proteger la privacidad y los datos personales de terceros a los que acceden durante el teletrabajo?

El teletrabajo no debe suponer ninguna merma en las obligaciones que respecto a las obligaciones de confidencialidad y secreto incumben al empleado cuando accede a datos personales.

Adicionalmente puede darse el supuesto de que durante las sesiones de teletrabajo se encuentren situaciones en que se realicen contactos con terceros que tienen el mismo

derecho a la protección de la privacidad. En este sentido sería aconsejable que el organizador remita a los participantes las recomendaciones indicadas en la pregunta anterior.

En la situación actual de confinamiento, se puede dar la circunstancia de que la privacidad y los datos personales de terceros a los que accede el empleado durante su jornada laboral puedan ser conocidos por el entorno familiar del empleado. En este supuesto el empleado deberá extremar las precauciones expresadas en la política de seguridad de la información, pudiendo adaptarse en su caso las previstas en cuanto al uso de BYOD. En cualquier caso, deberán establecerse criterios de acceso a los dispositivos como, por ejemplo, diferenciación de usuarios (cuenta específica para teletrabajar), uso de contraseñas, el bloqueo de pantallas y su desbloqueo mediante contraseñas, entre otras, y el resto de las indicadas en la política o normativa al respecto. Se debe valorar el uso de la audioconferencia o la omisión de la visualización de otros participantes. Si es posible, preferir el uso de auriculares sobre el de los altavoces internos o externos, así como evitar el uso de datos identificativos en las conferencias que puedan ser oídas por terceras personas.

En la misma línea de la pregunta anterior, solo se podrán utilizar aplicaciones corporativas debidamente licenciadas para que no se planteen problemas relevantes de protección de datos.

Pregunta 42: ¿Se puede controlar el teletrabajo?

El control del teletrabajo supone la adecuación de las actividades de tratamiento ya sea por la creación de un nuevo tratamiento cuya base de legitimación se encontraría en el art. 6.1.b) en relación con el art. 6.1.c), ambos del RGPD, o de la modificación de la ya existente.

Deben tenerse en cuenta las medidas adoptadas por los órganos competentes y, en su caso, las políticas de teletrabajo ya adoptadas siempre dentro del respeto a la protección de la intimidad del teletrabajo y sin que el teletrabajo suponga una merma en relación con el derecho al registro de la jornada laboral.

Cuando el teletrabajo se realice a través de dispositivos digitales aportados por la universidad solo se podrá acceder a los mismos "a los solos efectos de controlar el cumplimiento de las obligaciones estatutarias y de garantizar la integridad de dichos dispositivos" (art. 87.2 LOPDGDD). En el caso de que el teletrabajo se realice mediante dispositivos digitales aportados por el trabajador o funcionario, el acceso a dicho dispositivo no estaría permitido por cuanto resultaría desproporcionado, salvo cuestiones técnicas debidamente justificadas. En este sentido, afectaría al derecho fundamental a la intimidad personal.

Pregunta 43: ¿Cómo se puede controlar el teletrabajo ("fichaje") durante el estado de alarma?

Con carácter general debe descartarse la utilización de controles biométricos como el reconocimiento facial por existir métodos alternativos menos intrusivos. El control podría realizarse:

- Mediante el control de los accesos a las redes de las universidades (logs de conexión VPN) y a los recursos de la universidad utilizados para la gestión, como podría ser la conexión a teléfonos VoIP, a las bases de datos de gestión o a los escritorios de tramitación. Normalmente estos recursos requieren que se suministre un usuario y una contraseña única por cada uno de los empleados.

- También podría establecerse un sistema de fichaje telemático a través de una aplicación de fichaje.
- El uso de listados de trabajos y horario remitidos por el trabajador y validados por el responsable.

En todo caso, el sistema por el que se opte deberá respetar lo establecido en los arts. 87 a 91 LOPDGDD en cuanto al derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral (art. 87), el derecho a la intimidad frente al uso de videovigilancia y de grabación de sonidos en el lugar de trabajo (art. 89), el derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral (art. 90) y los derechos digitales en la negociación colectiva (art. 91).

Pregunta 44: ¿Cuál es la base de legitimación para el desarrollo de reuniones virtuales?

Como ya se ha expuesto, las circunstancias actuales y el Derecho aplicable a las mismas legitiman tanto el teletrabajo como los tratamientos que pudieran derivar de la nueva modalidad de prestación del servicio. Ello, consecuentemente, comporta la posibilidad de tratar los datos necesarios para desarrollar reuniones virtuales, con la misma base de legitimación (cumplimiento de obligaciones legales por parte de la universidad).

Las reuniones virtuales de trabajo entre personas empleadas pueden basarse adicionalmente en el art. 6.1.b) RGPD (ejecución de contrato -con carácter general, el consentimiento no es la base que legitima tratamientos de datos del personal-).

En el caso de los órganos colegiados, las reuniones podrán desarrollarse a distancia, en los términos previstos en sus estatutos o reglamentos internos. De no contar con previsiones específicas, parece aconsejable que los órganos de gobierno adopten iniciativas encaminadas a protocolizar las actuaciones y medios electrónicos dotados de las debidas medidas de seguridad, necesarios para la realización de sesiones telemáticas, a los efectos de garantizar la actividad de los mismos en las actuales circunstancias.

En el caso de las universidades públicas, el régimen aplicable es el establecido en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Los tratamientos derivados del desarrollo de las mismas tendrán como base de legitimación el art. 6.1.e) RGPD (misión realizada en interés público o ejercicio de poderes públicos). Y ello incluye la posible grabación de las sesiones (art. 18 Ley 40/2015).

En el caso de las universidades privadas, si sus estatutos o reglamentos internos no lo tuvieran previsto, hay que tomar las medidas extraordinarias aplicables a las personas jurídicas de Derecho privado previstas en el art. 40, apartados 1 y 2, del Real Decreto-Ley 8/2020.

Pregunta 45: ¿Cómo se debe cumplir con la obligación de informar en las reuniones virtuales?

Con carácter general, quienes participen en reuniones virtuales, al igual que los afectados cuyos datos se traten, son titulares de los derechos que el RGPD y la LOPDGDD les atribuyen (arts. 12 a 23 RGPD y arts. 11 a 18 LOPDGDD). La universidad debe asegurar el adecuado cumplimiento del deber de información o transparencia en los términos de los arts. 12 a 14 RGPD y 11 LOPDGDD con respecto a la persona empleada. Esta información puede facilitarse en el acuerdo de teletrabajo.

En cuanto al cumplimiento del deber de transparencia e información con respecto al tratamiento de los datos personales de los miembros de los órganos colegiados, podrán haber sido informados convenientemente al presentar su candidatura o al adquirir la condición por la que se integra en el órgano, si éste ya tenía prevista la posibilidad de reunirse a distancia. En caso contrario, será necesario informarles de las nuevas operaciones de tratamiento, incluyendo particularmente la posibilidad de que las reuniones puedan ser grabadas.

Pregunta 46: ¿La declaración del estado de alarma ha suspendido los plazos para notificar las brechas de seguridad a la AEPD o a la autoridad de control competente que corresponda? ¿y los plazos para atender las solicitudes de ejercicio de los derechos de los interesados en materia de protección de datos?

En caso de pérdida, sustracción o bloqueo ilícito de espacios en los que están alojados los datos personales o de cualquier otra brecha de seguridad que afecte a los ficheros, bases de datos y al tratamiento de los mismos, se debe comunicar inmediatamente al DPD dicha circunstancia, a través de los canales establecidos por la universidad, para que realice la oportuna valoración y adopte las medidas pertinentes, como sería la comunicación a la AEPD o a la autoridad de control competente en el plazo de 72 horas.

La suspensión de plazos administrativos prevista en Real Decreto 463/2020, por el que se declara el estado de alarma, no afecta a la obligación de notificar las quiebras de seguridad que afecten a datos personales.

Tampoco se han suspendido los plazos para dar respuesta al ejercicio de los derechos que el RGPD atribuye a las personas, con independencia de la naturaleza privada o pública del responsable del tratamiento ante el que se ejerzan. No obstante, el art. 12.3 RGPD permite prorrogar el plazo de respuesta de un mes por otros dos más, siempre que dicha prórroga se motive, por ejemplo, describiendo cómo afecta a la actividad del responsable la crisis del COVID-19. En esos casos, si no resultase viable notificar al interesado la prórroga en el plazo de un mes debido a las condiciones derivadas de la crisis podría realizarse, mediante una respuesta automática a la recepción de una solicitud de ejercicio de derechos.

7. Conclusiones

A modo de conclusión conviene señalar que las universidades, en el necesario proceso de adaptación acelerada de su funcionamiento a entornos digitales como consecuencia de la actual situación de crisis sanitaria, han de tener presente que la legislación de protección de datos personales y garantía de los derechos digitales se mantiene plenamente vigente. En este contexto, el objetivo de esta guía no es otro que servir de ayuda a los responsables y gestores de las universidades para llevar adelante este proceso con las debidas garantías.

Para garantizar el respeto de estos derechos, nuestro ordenamiento se ha dotado de la figura del Delegado/a de Protección de Datos. Esta figura, además de las funciones que explícitamente tiene atribuidas, puede y debe desempeñar un papel importante en la tarea de concienciar a la comunidad universitaria, también en un contexto como el actual, sobre la necesidad de prestar atención al respeto de estos derechos en el desarrollo de su actividad. Así pues, se hace indispensable contar con el asesoramiento de los DPDs en el diseño de las medidas que se adopten para solucionar las dificultades ahora generadas y que impliquen un tratamiento de los datos personales de, y por, los miembros de la comunidad universitaria.

Por lo que se refiere a la incidencia del derecho a la protección de los datos de carácter personal en la actividad docente, la actual situación no exime del respeto a la normativa aplicable. En consecuencia, la elección de las metodologías a utilizar debe tener en cuenta la importancia de utilizar las herramientas oficiales que proporcione la universidad, de manera que se pueda asegurar que el tratamiento de los datos personales se somete a las garantías técnicas y jurídicas adecuadas. Por otro lado, las singulares circunstancias en que se desarrollan actualmente las actividades docentes justifican que se puedan grabar para facilitar su seguimiento, si bien han de seguirse una serie de cautelas que se han explicado en las páginas anteriores.

En relación con los tratamientos de datos en los procesos de evaluación y su paso a modelos de evaluación online fruto de la actual crisis por el coronavirus, destacamos la necesidad de evaluar, controlar y evitar, o minimizar, el impacto que las metodologías empleadas tengan en la vida privada o en la expectativa de privacidad de los sujetos implicados en todas las fases del proceso de evaluación (antes, durante y tras la realización de las pruebas). Por ello, no sólo se debe extremar la obligación de información y de transparencia respecto de las medidas adoptadas, sino que además se hace imprescindible emplear las herramientas oficiales de nuestra institución, o bien, contar con una base de legitimación para poder tratar los datos estrictamente necesarios para la finalidad evaluadora perseguida, superando la necesaria predeterminación legislativa y la correspondiente evaluación de impacto, proceso en el que no puede faltar un DPD.

Para la investigación, una actividad que se integra en la propia naturaleza de la universidad, el cumplimiento de la normativa de protección de datos es esencial. Sólo habrá una investigación de calidad si es escrupulosa con los derechos fundamentales, entre los que se encuentra la protección de datos. Así las cosas, la pandemia del COVID-19 no altera en modo alguno la normativa de protección de datos, por lo que en la investigación universitaria hay que tener en cuenta su contenido. En él se hallan distintas previsiones específicas, no sólo de investigación en general, sino también en investigación en salud o biomédica. Los

investigadores deben tener una actitud proactiva para cumplir la normativa de protección de datos, actuar de manera leal y transparente con las personas interesadas, y articular las medidas técnicas y organizativas pertinentes para asegurar dicho cumplimiento.

En un contexto de teletrabajo, los riesgos para los derechos y libertades de las personas interesadas son esencialmente los vinculados a la seguridad dado que, en la cadena de medidas de seguridad de una organización, la parte más débil son las propias personas. Es esencial que las personas empleadas sean convenientemente informadas y formadas en el uso, exclusivo, de las herramientas provistas o permitidas por la institución, y concienciadas de los riesgos a los que se exponen, ellos y los sistemas de información, así como sobre la forma de comunicar de inmediato una brecha de seguridad. El teletrabajo no debe suponer ninguna merma en las obligaciones que respecto a las obligaciones de confidencialidad y secreto incumben a los empleados cuando acceden a datos personales, así como tampoco a su propia esfera de vida privada y familiar. Todo ello en un escenario en el que el objetivo común es proteger la salud de todos, lo cual nos lleva a tratar datos de salud, en el marco de planes de contingencia (prevención de riesgos laborales) o a requerimiento de las autoridades competentes.