

Guía de buenas prácticas en materia de Transparencia y Protección de Datos



Índice



	Página
01. Introducción	6
02. Guía de buenas prácticas en materia de transparencia y protección de datos	10
1. Estudiantes	11
2. Personas Fallecidas	22
3. Medios Tecnológicos	23
4. Imágenes	27
5. Actividad Investigadora y de Transparencia del Conocimiento	33
6. Información Económico-Financiera	41
7. Convenios	44
8. Procesos Electorales	45
9. Privacidad y Derecho de Defensa	47
10. Régimen Disciplinario	53
11. Publicación de Datos Personales	57
12. Personal	60
13. Órganos de Gobierno y Gestión Institucional	68
03. Anexo I. Glosario	72
04. Anexo II. Lista de abreviaturas	76
05. Anexo III. Documentación de interés	78



La publicación de la Ley 19/2013, de Transparencia, Acceso a la Información Pública y Buen Gobierno en diciembre de 2013; el Reglamento General de Protección de Datos, de plena aplicación desde mayo de 2018, así como la de la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales, el pasado mes de diciembre, hicieron necesario la posibilidad de contar con una Guía de buenas prácticas que recogiera las principales cuestiones recibidas en las Universidades sobre temas de transparencia y protección de datos.

La Guía que se presenta consta de 13 apartados y pretende dar respuesta a las cuestiones planteadas a través de la buena práctica de cada caso concreto. El texto, contemplado como un documento abierto, podrá ser objeto de actualización y de ampliación por el Grupo de trabajo de Protección de Datos –de reciente creación– con la finalidad de adaptarlo a las necesidades de las universidades, que irán surgiendo conforme se vaya aplicando la nueva legislación en protección de datos.

Quiero agradecer su colaboración a todas aquellas universidades que respondieron el cuestionario (54 universidades en total: 38 públicas y 16 privadas, de las 76 asociadas a Crue). Sin ellas no

habría sido posible la elaboración de esta Guía. También, quiero hacer extensible mi agradecimiento a la Agencia Española de Protección de Datos, en especial a Dña. Mar España, su directora, y a todo su equipo, por las facilidades aportadas. Y, por supuesto, al Grupo de Trabajo de Crue Universidades Españolas que ha elaborado este documento. No quiero finalizar esta introducción sin agradecer su dedicación y trabajo altruista a Dña. Francisca Fuentes, de la Universidad de Cádiz, y responsable del proyecto; al coordinador del proyecto, D. Francisco Manuel Barrera, de la Universidad de Granada; a Dña. María Ángeles Piedra, de la Universidad de Almería; a Dña. Juana María Zapata, de la Universidad Politécnica de Cartagena; y a Dña. Gloria Rodríguez, de la Fundación Universitaria San Pablo CEU.

Muchas gracias a todos los que han hecho posible este documento.

José Antonio Mayoral
Presidente de Crue-Secretarías Generales
Rector de la Universidad de Zaragoza

01



Introducción

El 10 de diciembre de 2013 aparece publicada en el BOE la Ley 19/2013, de Transparencia, Acceso a la Información Pública y Buen Gobierno en diciembre de 2013 cuyo objeto, expresado en su artículo 1, es “ampliar y reforzar la transparencia de la actividad pública, regular y garantizar el derecho de acceso a la información relativa a aquella actividad y establecer las obligaciones de buen gobierno que deben cumplir los responsables públicos así como las consecuencias derivadas de su incumplimiento” (artículo 1).

A partir de ese momento se hace necesario atender a las obligaciones previstas en la norma, tanto de publicidad activa como de derecho de los ciudadanos de acceso a la información pública, entendida ésta como “los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones” (artículo 13).

Este derecho de acceso, definido de una forma tan amplia, se va a ver limitado, sin embargo, en aquellos casos en que así sea necesario por la propia naturaleza de la información o por su entrada en conflicto con otros intereses protegidos. Entre ellos, y de forma relevante, se encuentra el derecho a la protección de los datos personales, por lo que la Ley aclara la relación entre ambos derechos estableciendo determinados mecanismos de equilibrio. Así, si en la medida en que la información afecte directamente a la organización o actividad pública del órgano prevalecerá el acceso, mientras que, por otro, para el acceso a los datos que la normativa califica como especialmente protegidos se requerirá, con carácter general, el consentimiento de su titular. Finalmente, señala la norma que cuando la información solicitada no contuviera datos especialmente protegidos, para conceder el acceso habrá que hacer una ponderación suficientemente razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada, en particular su derecho fundamental a la protección de datos de carácter personal, estableciendo determinados criterios para llevar a cabo dicha ponderación (artículo 15).

A tenor de estas disposiciones la situación en la práctica es que en la mayoría de las ocasiones no resulta fácil determinar cuándo prevalece el derecho de acceso y cuándo el de protección de datos de carácter personal, generándose dudas e incertidumbre en las respuestas a las solicitudes de acceso a la información.

En este escenario, en julio de 2017, Crue-Secretarías Generales encarga al Grupo de Trabajo de Gabinetes Jurídicos la elaboración de una Guía de buenas prácticas en materia de transparencia y protección de datos con el objetivo de ayudar a las universidades a la hora de responder a las solicitudes de acceso a la información pública recibidas.

Para llevar a cabo esta tarea se constituyó un grupo de trabajo que ha desarrollado una intensa labor en la que se han implicado los Gabinetes Jurídicos de todas las universidades españolas y que es de justicia exponer, aunque sea de manera muy breve.

El proceso de elaboración de la Guía se inició en septiembre de 2017 con el envío de un primer cuestionario a las universidades para una recogida inicial de información. Tras el análisis de la misma se procedió a una división del trabajo por materias y una planificación del mismo. En septiembre de 2018 se pidió de nuevo información a las universidades y tras ir recibiendo sus respuestas se fueron elaborando las distintas partes que integrarían la Guía. Cuando se tuvo una visión completa de lo que sería su contenido, y a la vista de las dudas que se suscitaban en diversas cuestiones, se solicitó una reunión con la AEPD, que se celebró en la sede de este organismo con la presencia de la Directora de la Agencia, Dña. Mar España, y distintas personas de su equipo. Tras esta reunión, y otras posteriores del Grupo de trabajo, se fue perfilando lo que sería el texto completo de la Guía, cuya redacción definitiva se concluyó en el mes de julio de 2019.

Se ha construido un documento basado en las cuestiones planteadas por las distintas universidades, a las que ha tratado de darse una respuesta siempre fundada jurídicamente, a tenor de la legislación vigente, de la jurisprudencia y de los



critérios establecidos por los distintos órganos de control en materia de transparencia y/o de protección de datos.

Obviamente, se trata de un documento abierto, sujeto a aportaciones, a revisiones, a modificaciones. Es una herramienta viva, que ha de evolucionar según vayan progresando desde el punto de vista jurídico las materias que en ella se contemplan (cambios normativos, nuevas sentencias, nuevas resoluciones de las agencias de control...) y que necesariamente habrá de ir ampliándose con la incorporación de supuestos no contemplados inicialmente.

Con él hemos tratado de dar respuesta al encargo que se nos hizo por parte de Crue-Secretarías Generales, y para cuyo cumplimiento hemos tenido una importante colaboración que es necesario recordar y agradecer.

Así, hay que comenzar por dar las gracias a los Gabinetes Jurídicos de todas las universidades españolas, cuya participación ha enriquecido este trabajo de una forma extraordinaria.

Un agradecimiento muy especial para los responsables de la Agencia Española de Protección de Datos, por su atención y su interés en esta Guía.

De forma muy particular hay que reconocer y agradecer el trabajo intenso, generoso, desinteresado y constante que han llevado a cabo Dña. María Ángeles Piedra Fernández, Directora del Gabinete Jurídico de la Universidad de Almería, Dña. Gloria Rodríguez Mármol, Delegada de Protección de Datos y Asesora Jurídica de la Fundación Universitaria San Pablo CEU, Dña. Juana María Zapata Bazar, Jefa de la Asesoría Jurídica de la Universidad Politécnica de Cartagena y D. Francisco Manuel Barrera López, Jefe de Servicio de los Servicios Jurídicos de la Universidad de Granada y coordinador del grupo de trabajo, cuyo impulso y liderazgo han contribuido de forma determinante a la elaboración de esta Guía.

Gracias, finalmente, a los Presidentes de Crue-Secretarías Generales, D. Salustiano Mato de la Iglesia, que nos encargó el trabajo, y D. José Antonio Mayoral Murillo, que lo ha apoyado firmemente, por la confianza depositada en el Grupo de Gabinetes Jurídicos para llevar a cabo esta tarea, y muy especialmente a D. Víctor Jiménez Jara, por la atención permanente y la ayuda prestada a las personas que han dedicado su tiempo y su esfuerzo a la misma.

Como se ha señalado, esta Guía tiene como objetivo principal servir de herramienta útil para la toma de decisiones de los responsables universitarios ante las solicitudes de acceso a la información pública. Adicionalmente, se ofrece un elenco de materias susceptibles de ser objeto de publicidad activa por parte de las universidades.

En ambos aspectos lo que se pretende con este documento no es más que servir de orientación a las universidades en su trabajo diario. El criterio que se ha de aplicar en cada caso es el que adopte cada universidad, dado que la Guía no tiene, como no podía ser de otra manera, carácter vinculante.

Personalmente, espero haber respondido en alguna medida al encargo que se hizo al Grupo de Trabajo de Gabinetes Jurídicos y agradezco enormemente haber podido colaborar con todas las personas y entidades que he citado, de las que tanto he aprendido y con las que tanto he compartido, personal y profesionalmente, en este proceso.

Francisca Fuentes Rodríguez
Presidenta del Grupo de Trabajo de Gabinetes Jurídicos de Crue-Secretarías Generales (julio 2017 - abril 2019)
Secretaria General de la Universidad de Cádiz (2012-2019)

RELACIÓN DE UNIVERSIDADES QUE CONTESTARON EL CUESTIONARIO

1. Universitat Abat Oliba CEU
2. Universidad de Alicante
3. Universidad de Almería
4. Universidad Antonio de Nebrija
5. Universitat Autònoma de Barcelona
6. Universidad Autónoma de Madrid
7. Universitat de Barcelona
8. Universidad de Burgos
9. Universidad de Cádiz
10. Universidad de Cantabria
11. Universidad Carlos III de Madrid
12. Universidad Católica San Antonio de Murcia
13. Universidad CEU Cardenal Herrera
14. Universidad CEU San Pablo
15. Universidad Complutense de Madrid
16. Universidad de Córdoba
17. Universidad de Deusto
18. Universidad Europea de Madrid
19. Universidad Europea Miguel de Cervantes
20. Euskal Herriko Unibertsitatea / Universidad del País Vasco
21. Universidad de Granada
22. Universidad de Huelva
23. Universitat de les Illes Balears
24. Universidad de Jaén
25. Universitat Jaume I
26. Universidad de La Rioja
27. Universidad de La Laguna
28. Universidad de Las Palmas de Gran Canaria
29. Universidad de León
30. Universitat de Lleida
31. Universidad de Mondragón
32. Universidad de Murcia
33. Universidad de Navarra
34. Universitat Oberta de Catalunya
35. Universidad de Oviedo
36. Universidad Pablo de Olavide
37. Universidad Politécnica de Cartagena
38. Universitat Politècnica de València
39. Universitat Pompeu Fabra
40. Universidad Pontificia Comillas
41. Universidad Pontificia de Salamanca
42. Universidad Pública de Navarra
43. Universitat Ramon Llull
44. Universidad Rey Juan Carlos
45. Universitat Rovira i Virgili
46. Universidad de Salamanca
47. Universidad San Jorge
48. Universidade de Santiago de Compostela
49. Universidad de Sevilla
50. UNED
51. Universitat de València
52. Universitat de Vic
53. Universidade de Vigo
54. Universidad de Zaragoza

02

Guía de buenas prácticas en materia de
transparencia y protección de datos

1. ESTUDIANTES

1.1. PUBLICIDAD ACTIVA¹

Oferta Académica

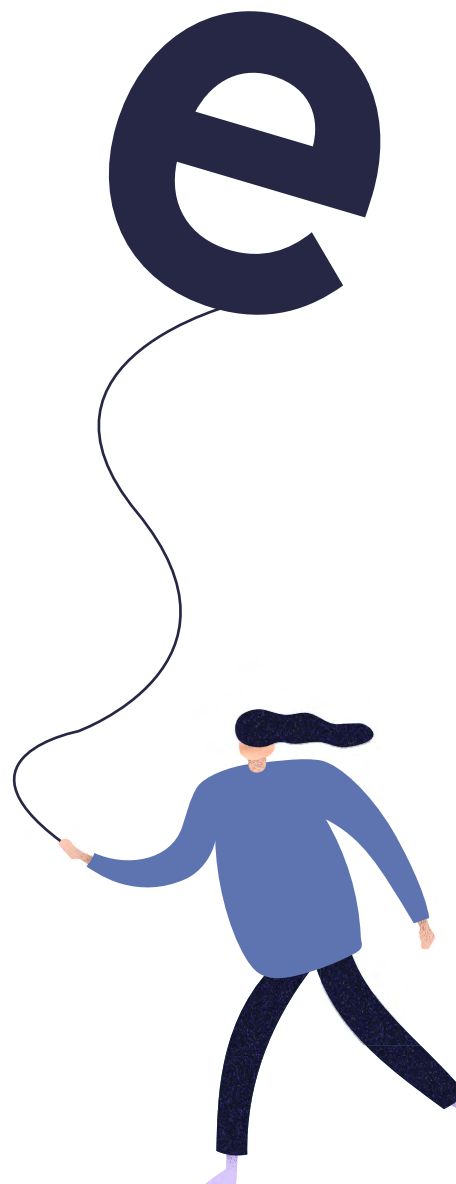
- Tipo (Oferta de titulaciones y planes de estudio):
 - Grado/Doble Grado
 - Máster/ Título Propio
 - Doctorado
 - Cursos de especialización
 - Ciclos formativos
 - Cursos de idiomas y acreditación lingüística
- Ramas de conocimiento, áreas y titulaciones asociadas:
 - Ciencias de la Salud
 - Artes y Humanidades
 - Ciencias Sociales y Jurídicas
 - Ciencias
 - Ingeniería y Arquitectura
- Centros

Datos relativos a los estudios universitarios y a los egresados

- Grado
- Posgrado

Admisión

- Admisión Grado
- Admisión Máster
- Admisión Doctorado
- Admisión Enseñanzas Propias
- Admisión Ciclos Formativos



¹ La información que se indica es orientativa, sin perjuicio del deber de adecuación de cada Universidad al marco normativo de transparencia que le sea de aplicación.

Ayudas y becas de las universidades

- Becas a los estudios de Grado
- Becas a los estudios de Posgrado
- Ayudas
- Premios

Servicios

- Prácticas y Empleo
- Biblioteca
- Orientación Psicológica
- Atención a estudiantes con necesidades especiales
- Vida en el Campus
- Alojamiento, residencias y colegios mayores
- Programas de movilidad nacional e internacional

Más datos de interés

- Evolución de la tasa de oferta y demanda de titulaciones
- Tasas de abandono escolar
- Evaluación y seguimiento de títulos y sistemas de garantía interna de calidad
- Indicadores de satisfacción del estudiantado
- Asociacionismo
- Voluntariado
- Teléfonos de interés y enlaces web

1.2. DATOS AGREGADOS

- *Solicitud de datos disociados de distinta índole (entre otros muchos, estadísticas de matriculaciones, tasas de rendimiento escolar, tiempo medio de tramitación de títulos)*

Se concede siempre que los datos sean agregados y, por tanto, anonimizados.

Las causas de inadmisión (entre ellas, las solicitudes repetitivas y abusivas, la acción previa de reelaboración y la información de carácter auxiliar o de apoyo) deben ser interpretadas atendiendo a los criterios establecidos por el Consejo de Transparencia y Buen Gobierno (en adelante, CTBG) y, en el caso de la aplicación de los límites al derecho de acceso a la información, en función de lo previsto en el criterio conjunto CTBG y la Agencia Española de Protección de Datos (en adelante, AEPD)².

1.3. ACCESO A DATOS ACADÉMICOS

Pueden darse diversos supuestos, entre los que cabe destacar:

- *Acceso por parte de los progenitores a los datos académicos de sus hijos*

En esta materia se ha pronunciado la AEPD en diversos informes (0036/2018; 0141/2017; 0441/2015; 0178/2014). Para la existencia de presunción de interés legítimo habría que acreditar que se abona la pensión alimenticia o la dependencia económica. Señala la AEPD que “el criterio de dependencia eco-

² Pueden consultarse todos ellos mediante los enlaces incluidos en el anexo III de la presente guía.

nómica, debe examinarse en cada caso, si bien en principio está referida a que se abone una pensión de alimentos o se financien los gastos de subsistencia del interesado por ambos progenitores o por uno de ellos, en tal caso, el interés legítimo lo ostentará únicamente aquél progenitor de quien sea económicamente dependiente”

Cuando se trata de la modificación de la pensión de alimentos, la AEPD considera que “[...] parecen darse los elementos que permiten que la comunicación de los datos sea conforme a lo previsto en el artículo 6.1.f del Reglamento, en tanto que existe un interés legítimo en el progenitor fundado en el derecho que el artículo 152 del Código civil le reconoce, el conocimiento de tales datos resulta necesario para satisfacer ese interés legítimo, toda vez que tal información debe aportarse como prueba en un procedimiento judicial y tal derecho parece prevalecer sobre los intereses y derechos y libertades del interesado, sin que ello obste a que éste pueda ejercer su derecho de oposición a tal tratamiento, debiendo examinarse si las circunstancias alegadas quiebran tal presunción de existencia de un interés legítimo” (informe 0036/2018)³.

Por consiguiente, deberá examinarse, caso a caso:

- a) El concreto interés legítimo que ostenta quien solicita los datos.
- b) Si el conocimiento de los datos que constan en la Universidad es necesario para la finalidad perseguida por aquél.
- c) Si el interés legítimo ostentado ha de prevalecer sobre los derechos y libertades del interesado, al que debe informarse a fin de que pueda ejercer su derecho de oposición, si lo estima procedente, al tratamiento. Por ejemplo, no existiría en principio esa presunción de interés legítimo si el estudiante mayor de edad acredita que es independiente económicamente y ha decidido voluntariamente no mantener relaciones con sus progenitores.



Buena práctica: requerir siempre el último ingreso abonado antes de la solicitud, para evitar supuestos en los que se haya dejado de satisfacer la pensión alimenticia, además de la resolución judicial correspondiente.

En el caso de menores de edad no emancipados (art. 154 CC), toda vez que la facultad de acceso a la mencionada información se encuentra dentro del marco de los deberes y derechos que corresponden a los padres, inherentes al ejercicio de su patria potestad, la obligación de educación de los progenitores hacia sus hijos ampara la cesión de los datos académicos del menor, tal y como se recuerda por la AEPD (informe 0466/2004), salvo que en virtud de resolución judicial se excluya el ejercicio de la patria potestad (informe 0227/2006), o existan circunstancias excepcionales concurrentes en un caso concreto, declaradas mediante resolución judicial, que implique la mayor prevalencia del derecho a la protección de datos del menor.

En idéntica situación estaría el supuesto de aquella persona que ostenta la patria potestad o tutela del estudiante (por incapacidad declarada judicialmente), siempre que se aporte la correspondiente resolución judicial (art. 199 CC), salvo que, por las circunstancias concretas del caso, deba prevalecer el derecho a la protección de datos.

³ En análogo sentido, véase resolución TD/00013/2019 de la citada Agencia.

- *Comunicación a instituciones públicas o privadas que tienen suscritos acuerdos de colaboración con la Universidad para la concesión de becas a los estudiantes*

La cesión será posible en cumplimiento del correspondiente acuerdo de colaboración, sin perjuicio del deber de informar a los solicitantes –art. 13 del Reglamento (UE) 2016/679, de 27 de abril de 2016 (en adelante, RGPD)- en las bases de cada convocatoria, y siempre que se atienda a los principios de limitación de la finalidad y de minimización -artículos 5.1.b) y 5.1.c) RGPD, respectivamente-.

- *Comunicación a empresas e instituciones que pretenden contratar a egresados o estudiantes*

La comunicación de datos a empresas e instituciones que pretenden contratar a egresados o estudiantes debe basarse en el consentimiento del interesado.



Buena práctica: requerir al afectado que confirme a través de correo electrónico la autenticidad de la autorización a la entidad o empresa en caso de que no se aporte con la solicitud copia del documento identificativo del egresado o estudiante.

- *Datos académicos de cargos públicos*

En el ámbito universitario parece razonable circunscribir el concepto de cargo público, a falta de una regulación expresa, a los titulares de los órganos de gobierno y representación de las universidades públicas previstos en el artículo 13 b) de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades (en adelante, LOU) y los que tengan tal consideración en función de lo establecido en las normas de organización y funcionamiento de las universidades privadas (art. 27.1 LOU).

Por ello, cuando se solicite el acceso a datos académicos de un cargo público, en principio habría prevalencia del interés general en el conocimiento de la preparación académica de quienes asumen los más altos puestos en la estructura administrativa -art. 6.1.f) RGPD-, atendiendo en cualquier caso a los principios de minimización -art. 5.1.c) RGPD- y de limitación de la finalidad -art. 5.1.b) RGPD-.



Buena práctica: el currículum académico de las citadas personas debería de hacerse público en los portales de transparencia, en aquellos supuestos en los que no sea objeto preceptivo de publicidad activa.

- *Comunicación o cesión de datos académicos entre unidades de la misma Universidad o entre administraciones públicas*

El tratamiento de datos por otras unidades de la misma Universidad no tiene la consideración jurídica de “comunicación o cesión” en términos de protección de datos. Sería lícita siempre que se respete y se limite el acceso a aquellas personas en la medida en que lo necesiten para cumplir con las funciones que tienen atribuidas.

Respecto a las cesiones de datos entre Administraciones públicas, debemos estar a lo establecido en el informe de la AEPD 0175/2018 que determina lo siguiente:

- a. “[...] No cabe un acceso masivo e indiscriminado a datos personales, y por lo tanto, en cambio, cuando exista la posibilidad de cesión establecida en una ley, dicho acceso deberá ser siempre ‘específico en cada caso ajustado a los datos que resulten precisos para la tramitación de un expediente determinado y no de un acceso masivo e indiscriminado’; ‘tal acceso sólo podría producirse cuando ese dato

resulte necesario o pertinente en relación con la tramitación de un concreto expediente, lo que permite analizar o determinar en cada caso la conformidad del acceso con lo establecido en el régimen General que le resulte de aplicación” (STC 19/2013, de 31 de enero, FJ 7º) (RTC 2013/17).

- b.** *La cesión será lícita “si dichos datos se utilizan para un fin que no sea distinto; es decir, no se altera la finalidad”. Asimismo, “[...] habrá de tener en cuenta la legislación especial que pueda determinar una restricción a las cesiones de datos personales”.*
- c.** *Cuando la finalidad sea distinta, habrá que ver en primer lugar “si existe una norma de Derecho de la Unión o del Estado miembro que permita el tratamiento de los datos para salvaguardar los objetivos del art. 23.1 RGPD”. Por consiguiente, “el tratamiento basado en la misma sería ‘lícito’, por disposición del propio RGPD aun cuando su finalidad fuese incompatible con la finalidad para la que se recogieron los datos inicialmente”.*

Si “dicha norma no existe, o no fuese aplicable al caso [...] habría que realizar “una ponderación en los términos del art. 6.4, apartados a) a e) [RGPD]”, u otros razonables, ya que los incluidos en el citado precepto no constituyen una lista cerrada y exhaustiva. Si sobre la base de dichos criterios, y para cada caso concreto, se considera que el fin para el que se utilizarían los datos personales cedidos es compatible con el fin inicial, podrían cederse dichos datos.

Un ejemplo de tratamiento lícito sería el acceso pretendido por un profesor a los datos académicos de los estudiantes a los que imparte docencia. En este caso, no será necesario el consentimiento de aquellos, ya que se trataría del interés público consistente en la preservación del adecuado seguimiento de su aprendizaje –art. 6.1.e) RGPD-, si bien el acceso debe ser acorde con el principio de minimización de datos.

Por el contrario, el acceso por parte de un profesor a los datos académicos de los estudiantes (entre otros, asignaturas matriculadas, calificaciones) a los que no imparte docencia requerirá el previo consentimiento de los interesados, salvo que resulte de aplicación cualquier otra base de legitimación.

Por su parte, no sería acorde con el principio de minimización el acceso a los nombres y apellidos de los estudiantes que han superado el TFM o el TFG para presentación de méritos a evaluar por la ANECA por parte de un profesor, ya que ese dato no es necesario para obtener la evaluación. Por ello, sería suficiente, a los efectos que se pretenden, que se certificara de forma disociada las calificaciones obtenidas en los trabajos dirigidos y, en su caso, el título del trabajo en cuestión. En la última versión de la guía de la ANECA (2018) no se alude a la exigencia de tal dato personal en estos certificados.

- *El solicitante no puede acreditar interés legítimo, o aun estando acreditado, no prevalece sobre el derecho a la protección de datos*

El acceso a los datos académicos (entre ellos, calificaciones, títulos) solo puede realizarse si concurre alguna de las bases jurídicas de legitimación del artículo 6 del RGPD.

- *Acceso a datos de becas y ayudas al estudio concedidas*

La publicación del listado de beneficiarios (nombre y apellidos), con indicación del importe de la beca concedida a estudiantes tiene suficiente habilitación en normas con rango legal -art. 20.8 de la Ley 38/2003, de 17 de noviembre, General de Subvenciones, y art. 8.1.c) de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (en adelante, LTAIBG), o

la correspondiente ley autonómica de transparencia-, por lo que no es necesario disponer del consentimiento de los afectados, al prevalecer el interés público en su conocimiento, siempre atendiendo al principio de minimización y a lo previsto en la Disposición Adicional Séptima de la [Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales](#) (en adelante, LOPDGDD), tal y como se indica en la [Orientación para la aplicación provisional de la Disposición Adicional Séptima de la LO 3/2018](#), aprobada por la AEPD.

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

No obstante, hay que tener en cuenta que determinadas ayudas socioeconómicas pueden tener como objeto la atención a personas en situación de vulnerabilidad social, por lo que, como indica la Autoridad Catalana de Protección de Datos (en adelante, APDCat), debe preservarse la identidad de los beneficiarios, aplicando para ello lo dispuesto en el art. 46 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, (en adelante, LPACAP) ([dictamen CNS 28/2015](#)).

- [Acceso a datos académicos por parte de medios de comunicación](#)

La relevancia pública de una persona es un criterio que, salvo que se acredite unas circunstancias excepcionales concretas, hace que prevalezca el interés público –art. 6.1.e) RGPD- en el acceso a la información curricular, considerando que al representante público debe exigírsele, como parte sustancial de su proyección y relevancia institucional, la máxima transparencia de su perfil académico y profesional.

No obstante lo anterior, se ha de atender en cualquier caso al principio de minimización, sin que se deba facilitar información que no tenga una incidencia manifiesta en la notoriedad del escrutinio público.

Por ello, en este punto, lo importante no es en calidad de qué condición se solicita el acceso a la información pública sino el interés público o no de la misma, por lo que resultan de aplicación los criterios indicados para el acceso a datos académicos de cargos públicos.

1.4. ACCESO AL CONTENIDO DE TRABAJOS FIN DE GRADO (TFG) O FIN DE MÁSTER (TFM)

El acceso a estos trabajos requiere del consentimiento expreso del autor, salvo que se establezca lo contrario en la normativa específica de cada Universidad, dejando a salvo siempre sus derechos de propiedad intelectual.



Buena práctica: que, cuando se requiera el consentimiento, en los acuerdos de difusión electrónica en los repositorios institucionales y de difusión en internet se permita manifestar el consentimiento expreso de aquellos interesados en que su trabajo sea de conocimiento público.

Cuando se trate de un cargo público, en principio habría prevalencia del interés general en el conocimiento de la citada información, como se ha indicado en el [subepígrafe 1.3](#), dejando a salvo siempre los derechos de propiedad intelectual del autor.



1.5. ACCESO AL CONTENIDO DE LOS EXÁMENES

Las respuestas por escrito dadas en un examen y las eventuales anotaciones del examinador referentes a esas respuestas son datos personales, atendiendo en identidad de razón al pronunciamiento contenido en la *STJUE de 20 de diciembre de 2017*, as. C-434/16, *Nowak y Data Protection Commissioner*, por lo que el estudiante que ha efectuado el examen tiene derecho de acceso a la citada información (art. 15 RGPD).

1.6. PUBLICACIÓN DE LOS LISTADOS CON LAS CALIFICACIONES DE LOS ESTUDIANTES

La AEPD aclara en su *informe 0030/2019* que la publicación de las calificaciones universitarias tiene su base de legitimación en el art. 6.1.e) RGPD pero también en el art. 6.1.f) RGPD porque *“aun no tratándose los procedimientos de evaluación de procedimientos de concurrencia competitiva, las calificaciones obtenidas van a tener incidencia [...] en el otorgamiento de las matrículas de honor limitadas a un número de estudiantes, así como también en la concesión de premios extraordinarios, por lo que también podría apreciarse un interés legítimo de los alumnos del grupo en el conocimiento de las calificaciones de sus compañeros”*.

- *Publicación en la intranet institucional*

Se debe utilizar, como medio preferente, la intranet o plataformas docentes oficiales de cada institución universitaria para proceder a la publicación de las calificaciones, estando limitado el acceso a los profesores y compañeros del grupo.

- *Publicación en tabloneros físicos*

En el caso de que la publicación en la intranet no garantice el conocimiento por todos los estudiantes de sus calificaciones y de las de los compañeros de grupo, podrá realizarse en el tablón de anuncios físico del centro o departamento, siempre que se atienda a las siguientes pautas:

- a) No se encuentren en las zonas comunes de los centros (pasillos, etc.).
- b) Se garantice que el acceso a los mismos queda restringido a dichas personas.
- c) Se adopten las medidas necesarias para evitar su público conocimiento por quienes carecen de interés en el mismo.

Se procurará preservar la documentación a través de tabloneros cerrados con llave y, si no es posible, se monitorizará la información personal publicada evitando que la documentación pueda ser retirada por personas no autorizadas.

- *Normas comunes para ambos modos de publicación (electrónica y física)*

En cualquier caso, se deberá atender al principio de minimización, por lo que se harán públicos solos los datos que sean estrictamente necesarios para el ejercicio de la finalidad que se pretende (el conocimiento por los interesados de las calificaciones obtenidas), sin incluir mención al DNI o documento equivalente, salvo que hubiera coincidencia de estudiantes con los mismos nombres y apellidos o exista norma que exija la publicación del número del documento de identificación, en cuyo caso se actuará de conformidad con las previsiones contenidas en la *Orientación para la aplicación provisional de la Disposición Adicional Séptima de la LO 3/2018*.

En cuanto al tiempo en el que deberá mantenerse dicha publicación, en el caso de las calificaciones provisionales lo será mientras transcurre el plazo para presentar reclamaciones, y respecto a las calificaciones definitivas durante el tiempo imprescindible que garantice su conocimiento por todos los interesados.



Buena práctica: si se utiliza cualquier otro medio para comunicar las calificaciones (entre ellos, sistemas de mensajería instantánea, dispositivos electrónicos) hay que adoptar las debidas precauciones que garanticen la integridad y confidencialidad. En este sentido, no se aconseja comunicar las calificaciones por teléfono, por el riesgo potencial que conlleva una posible usurpación de la identidad, salvo que haya suficientes garantías de verificación de que la persona con la que se está comunicando es quién dice ser.

Buena práctica: incluir un texto explicativo en los listados y actas indicando que el destinatario de la información no puede difundir o usar los datos personales de los que ha tomado conocimiento sin estar autorizado previamente por el titular de los datos personales, siendo a todos los efectos responsable en caso de incumplimiento.

Buena práctica: que las unidades de tecnologías de la información y comunicación de las universidades desarrollen medidas que permitan el acceso universal de los usuarios a sistemas de consulta por intranet corporativa con el objeto de que en la regulación normativa de cada institución universitaria se elimine la opción de publicación en tableros físicos.

1.7. PUBLICACIÓN DE LISTADOS CON DATOS PERSONALES DE LOS ESTUDIANTES

Resulta aconsejable la publicación en la intranet institucional, al minimizar el riesgo potencial de acceso por parte de personas no autorizadas, si se utilizan adecuados protocolos de seguridad. Solo ha de tener acceso a la documentación con datos personales las personas afectadas (por ejemplo, los solicitantes de una línea de investigación del TFM). Por lo demás, se atenderá a las recomendaciones indicadas en el [subepígrafe 1.6](#).

1.8. DATOS DE CONTACTO

● *Contacto solicitado por el profesorado*

La solicitud, por parte de un profesor, de acceso a los datos de contacto de un estudiante que no pertenece al grupo de su clase (entre ellos, correo electrónico, teléfono) requiere del previo consentimiento del afectado.

● *Contacto para reunión de promociones*

El acceso a los datos de contacto para organización de reuniones para celebrar el aniversario de egresados de una promoción requerirá del previo consentimiento de los afectados.

● *Contacto solicitado por los delegados de estudiantes*

En este caso habría que distinguir varios supuestos:

a) Cuando los datos de contacto son solicitados por la Delegación de Estudiantes de la propia Facultad o Escuela habría un interés público -art. 6.1.e RGPD- siempre que la finalidad se limite exclusivamente a mantener informado a sus representados en el marco de las competencias atribuidas a estos órganos universitarios.



Buena práctica: sustituir el envío masivo a direcciones de correo electrónico por medios menos intrusivos, y acordes con el principio de minimización, como la creación de una lista de distribución.

b) Cuando los datos de contacto son solicitados por una Delegación de Estudiantes de una Facultad o Escuela distinta, no existiría interés público teniendo en cuenta que no es el órgano competente para representar a esos estudiantes, por lo que en este caso se requeriría el previo consentimiento de los afectados.



Buena práctica: que el delegado haga público su correo de contacto para que aquellos estudiantes que lo deseen contacten con esta persona.

c) Cuando los datos de contacto son solicitados por un delegado de clase y se extiende al conjunto de sus compañeros de grupo, habría un interés público -art. 6.1.e RGPD- siempre que la finalidad se limite exclusivamente a mantener informado a sus representados en el marco de las competencias que la Universidad le haya atribuido.



Buena práctica: sustituir el envío masivo a direcciones de correo electrónico por medios menos intrusivos, y acordes con el principio de minimización por la creación de una lista de distribución.

d) Cuando los datos de contacto son solicitados por un delegado de clase y se extiende al conjunto de estudiantes de varios grupos, no existiría interés público teniendo en cuenta que no es el órgano competente para representar a esos estudiantes, por lo que en este caso se requeriría el previo consentimiento de los afectados.



Buena práctica: que el delegado haga público su correo de contacto para que aquellos estudiantes que lo deseen contacten con esta persona.

En cualquier caso, cualquier dato de contacto que se facilite debe ser conforme con el principio de minimización, limitándose por ello al correo electrónico facilitado por la institución a sus estudiantes.

1.9. INFORMACIÓN DE INTERÉS ACADÉMICO

• *Envío de información relativa a estudios que imparte la Universidad*

El envío de información de interés académico a estudiantes, egresados y antiguos estudiantes requeriría del previo consentimiento de los afectados. En el caso de los egresados o antiguos estudiantes, será válido el consentimiento expreso que hubieran prestado cuando mantenían su vinculación académica con la Universidad, para continuar recibiendo esa información una vez finalizados los estudios, siempre que en ambos supuestos se ajuste a los términos previstos en el RGPD.



Buena práctica: en el caso de los egresados o antiguos estudiantes que se recabe el consentimiento expreso para recibir información de interés universitario antes de que finalicen sus estudios.

Buena práctica: canalizar este tipo de información de interés académico a través de canales de suscripción o “newsletter”.

1.10. PRÁCTICAS

- *Comunicación a centros externos de los datos personales relativos a la no comisión de delitos sexuales para la realización de prácticas en sus instalaciones y que impliquen contacto habitual con menores*

Se recaban los certificados negativos de comisión de delitos sexuales de los estudiantes de la Universidad que, en el desempeño de sus prácticas, tengan relación con menores de edad y se expiden acreditaciones a los centros educativos haciendo constar que el estudiante ha aportado el preceptivo documento. Este tratamiento de datos se fundamenta en la Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia, que recoge como obligatorio que todos los profesionales que trabajen con menores de forma habitual presenten un certificado negativo de antecedentes penales relativos a delitos sexuales. Se está, por tanto, ante el cumplimiento de una obligación legal -art. 6.1.c) RGPD-.



Buena práctica: que se suscriban instrumentos convencionales que aseguren la interoperabilidad y seguridad de la citada información entre las universidades y el Ministerio de Justicia, con garantía de la protección de los datos de carácter personal.

- *Comunicación de datos personales de estudiantes que van a realizar prácticas a una empresa o institución*

La cesión será posible siempre que se cumpla algunas de las condiciones de licitud recogidas en el artículo 6 RGPD, como podría ser el cumplimiento del correspondiente acuerdo de colaboración, el interés público o el consentimiento del interesado, sin perjuicio del deber de informar a los estudiantes, y de cumplir el resto de principios recogidos en el art. 5, como el de limitación de la finalidad, el de minimización y de seguridad.

No hay encargo de tratamiento pues cada parte será responsable del tratamiento de los datos del estudiante en la medida en que sea necesario para el adecuado desarrollo de las obligaciones estipuladas en el convenio o acuerdo, garantizando el cumplimiento del RGPD.

1.11. CATEGORÍAS ESPECIALES DE DATOS

El tratamiento de categorías especiales de datos tiene que estar legitimado en alguno de los títulos habilitantes contenidos en el art. 9.2.1 RGPD y, acumulativamente, en algunas de las condiciones de licitud recogidas en el art. 6.

1.12. DATOS IDENTIFICATIVOS

- *Preuniversitarios que participan a través de convenio con su centro educativo en actividades y concursos organizados por escuelas y facultades*

El tratamiento se legitima en el interés público -art. 6.1.e RGPD-. En cualquier caso, hay que informar a los interesados del tratamiento de sus datos.



Buena práctica: incluir en la convocatoria o en las bases del concurso la finalidad del tratamiento y las responsabilidades que asume cada parte en materia de protección de datos, sin perjuicio de la información que hay que facilitar a los interesados en base al art. 13 RGPD.

- *Cesión de datos para préstamo interbibliotecario*

Dicha cesión estaría amparada tanto en el cumplimiento de los convenios interbibliotecarios (interés público), como en el propio consentimiento del estudiante que solicita dicho servicio, atendiendo siempre al principio de minimización.

- *Solicitud del listado de estudiantes, junto a sus fotografías, que finalizaron sus estudios en un determinado año*

El solicitante debería acreditar alguno de los títulos habilitantes de los recogidos en el art. 6 RGPD para el tratamiento de los datos, como podría ser el previo consentimiento de las personas afectadas o un interés legítimo, debidamente acreditado, que sustentara la petición de su solicitud y que prevaleciera sobre el derecho de protección de datos.

1.13. SEGUROS

- *Cesión de los datos para entidad aseguradora*

El solicitante debería acreditar uno de los títulos habilitantes de los recogidos en el art. 6 RGPD, como podría ser el cumplimiento de una relación contractual.

1.14. FUERZAS Y CUERPOS DE SEGURIDAD

- *Solicitud de datos personales de estudiantes de la Universidad por parte de las Fuerzas y Cuerpos de Seguridad del Estado*

Siguiendo el criterio de la AEPD (entre otros, [informe 0133/2008](#) sobre cesión de datos a la Policía Judicial la comunicación de datos a la Policía Judicial sería lícita, siempre y cuando se cumplan las siguientes condiciones:

- a. Que quede debidamente acreditado que la obtención de los datos resulta necesaria para la prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales y que, tratándose de datos especialmente protegidos, sean absolutamente necesarios para los fines de una investigación concreta.
- b. Que se trate de una petición concreta y específica, al no ser compatible con lo señalado anteriormente el ejercicio de solicitudes masivas de datos.
- c. Que la petición se efectúe con la debida motivación, que acredite su relación con los supuestos que se han expuesto.
- d. Que, en cumplimiento del artículo 22.4 de la Ley Orgánica 15/1999, los datos sean cancelados "cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento".

En el caso de que haya mandamiento judicial o requerimiento de la Fiscalía la base de legitimación es el art. 6.1.c) RGPD, ya que existe un deber de colaboración con los Juzgados y Tribunales o con el Ministerio Fiscal (art. 236 quáter de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y art. cuarto cinco de la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal)⁴.

Otra cuestión que se puede plantear es si la Universidad podría ceder datos de sus estudiantes a las Fuerzas y Cuerpos de Seguridad del Estado, en cualquier caso, aunque no actué en funciones de Policía Judicial. La respuesta en este caso debe de ser negativa si no se acredita que los datos personales solicitados son necesarios para la prevención de un peligro real para la seguridad pública y se trata de una petición concreta y específica.



Buena práctica: no atender peticiones de documentación solicitadas verbalmente y aquellas que sean genéricas, sin perjuicio de requerir la correspondiente subsanación.

⁴ Puede consultarse asimismo el Dictamen 3/13, de la Abogacía del Estado.

2. PERSONAS FALLECIDAS

2.1. CUENTAS DE CORREO PROFESIONALES

- *Acceso al contenido de la cuenta de correo electrónico profesional de una persona fallecida, al acreditar ser su heredero o heredera*

No se facilitaría el acceso cuando existen datos de terceras personas en los contenidos de los correos. Además, se debe tener en cuenta que se está ante una herramienta profesional de titularidad de la Universidad.

2.2. HISTORIAL ADMINISTRATIVO

- *Acceso a determinada información (por ejemplo, número de trienios reconocidos) del historial administrativo de una persona fallecida por persona vinculada por razones familiares o de hecho*

De conformidad con lo previsto en el artículo 3 LOPDGDD, se facilita el acceso, salvo que la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley.

2.3. HISTORIAL ACADÉMICO

- *Acceso al expediente académico de un estudiante fallecido por sus progenitores, previa acreditación del vínculo*

De conformidad con lo previsto en el artículo 3 LOPDGDD, se facilita el acceso, salvo que la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley.

2.4 HISTORIAS CLÍNICAS

Solo se facilitará el acceso a la historia clínica custodiada en el correspondiente servicio o unidad de salud y prevención laboral de los pacientes fallecidos a las personas vinculadas a él, por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite.

En cualquier caso, el acceso de un tercero a la historia clínica motivado por un riesgo para su salud se limitará a los datos pertinentes. No se facilitará información que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros (art. 18.4 de la 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).



3. MEDIOS TECNOLÓGICOS

3.1. APLICACIONES PARA DISPOSITIVOS MÓVILES

- *Acceso a datos de los estudiantes por parte de la entidad que da soporte a la aplicación móvil de la Universidad*

El acceso a los datos personales de los estudiantes (entre otros, datos académicos, de contacto) no requerirá el consentimiento del afectado siempre que se realice en su condición de encargado de tratamiento y se ajuste estrictamente a las condiciones estipuladas en el contrato de encargo (art. 28 RGPD).

En cuanto a las posibles utilidades comerciales de la aplicación, será necesario el previo consentimiento del estudiante al no entrar este supuesto en las finalidades propias de la institución universitaria.

3.2. APLICACIONES DE MENSAJERÍA INSTANTÁNEA

- *Se pretende constituir un grupo de WhatsApp en el que participen los delegados y los estudiantes*

Se requiere el consentimiento de cada uno de los que vayan a participar o unirse al grupo ya creado, al no entrar este supuesto en las restantes bases jurídicas de legitimación del tratamiento. No existe un interés público en que cada persona participante conozca los teléfonos del resto.



Buena práctica: resulta recomendable, como se ha indicado en el epígrafe de “estudiantes”, que la comunicación entre delegados y estudiantes, siempre que los primeros actúen en el desempeño de sus funciones, se realice mediante medios técnicos establecidos por la Universidad (por ejemplo, a través de una lista de distribución).

- *Creación de grupos entre profesores y estudiantes con aplicaciones de mensajería instantánea*

Se requiere el consentimiento de cada uno de los que vayan a participar en el grupo, al no entrar este supuesto en las restantes bases jurídicas de legitimación del tratamiento.



Buena práctica: resulta recomendable que se empleen los medios técnicos establecidos por la Universidad (por ejemplo, uso de plataformas institucionales de apoyo a la docencia o listas de distribución).

3.3. DIRECCIONES IP

- *Acceso de un miembro de la comunidad universitaria a las direcciones IP desde las que se hayan podido conectar a su cuenta profesional, ante la sospecha de que un tercero ha podido efectuar una entrada indebida*

Se pretende discriminar los accesos producidos, al detectarse un posible uso indebido de su cuenta.

No procede el citado acceso, puesto que la indagación o investigación del posible acceso indebido corresponde realizarla a los propios servicios informáticos de la Universidad cuando se trata de recursos tecnológicos propiedad de la institución, quienes elevarán sus conclusiones a las autoridades competentes de la Universidad para poner, en su caso, los hechos en conocimiento de las autoridades competentes para la averiguación y persecución de posibles ilícitos.

Todo ello, sin perjuicio de las medidas correctoras que la persona interesada pueda adoptar (cambios de contraseña, etc.). Asimismo, el afectado puede también poner los hechos en conocimiento de las autoridades competentes para la averiguación de posibles ilícitos.

3.4. LISTAS DE DISTRIBUCIÓN

- *Solicitud de baja de las listas de distribución de la Universidad*

En las listas de naturaleza institucional (aquellas creadas para divulgación de las noticias de interés general para los miembros de la comunidad universitaria), el ejercicio del derecho de oposición, y el consecuente cese en el tratamiento de los datos personales, haría perder a estas su propia finalidad.

En lo que respecta a las listas específicas creadas para incluir a colectivos singularizados con interés común sobre un tema concreto (integrantes de grupos de investigación, delegaciones de estudiantes, entre otros), debe prevalecer, con carácter general, el derecho de oposición de la persona interesada (art. 21.1 RGPD). Este mismo derecho ha de extenderse a las listas creadas para difusión de información sindical⁵, excepto en los periodos electorales, como ha reiterado la AEPD (por todas, resoluciones TD-0119-2008; TD- 00869-2014; TD-002429-2017).

En cuanto a los servicios de “newsletter” (boletines de noticias), que la universidad pueda ofrecer a cualquier ciudadano, al fundamentarse su base legitimadora en el consentimiento expreso -art. 6.1.a) RGPD y art. 21 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico-, el interesado tiene el derecho a revocar su consentimiento en cualquier momento, por lo que de ejercerse este derecho tendría que ser dado de baja.



Buena práctica: una vez tramitada la baja, se remitirá automáticamente un mensaje de correo electrónico al solicitante para que la confirme, y evitar así posibles accesos indebidos de terceros que podrían suplantar la identidad del solicitante de la baja.

3.5. GEOLOCALIZACIÓN EN EL ÁMBITO LABORAL

De conformidad con lo dispuesto en el artículo 90 de la LOPDGDD, los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores (en adelante, TRLET) y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.

Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos⁶. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

⁵ La remisión de información a través del correo electrónico estaría amparada en el derecho a la libertad sindical. Por todas, véase la STC núm. 281/2005, de 7 de noviembre (RTC 2005\281).

⁶ Puede consultarse la resolución de la AEPD AP/00061/2018. En la jurisprudencia, entre las más recientes, la SAN núm. 136/2019, de 6 de febrero (AS 2019\905).

3.6. USO DE DISPOSITIVOS DIGITALES EN EL ÁMBITO LABORAL

- *Acceso a los contenidos derivados del uso de medios digitales por parte del empleador*

De conformidad con lo dispuesto en el artículo 87 de la LOPDGDD, los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.

El empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.

Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores.

El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados⁷. En este sentido, la LOPDGDD ha venido a dar naturaleza legal a la doctrina jurisprudencial en la materia (por todas, STS núm. 966/2006, de 26 de septiembre) (RJ 2007\7514).

Es importante recordar que los trabajadores deberán ser informados de los citados criterios de utilización.

3.7. BLOG

- *Publicación en blog de un profesor de las calificaciones de los estudiantes*

El blog de un profesor es un medio de información y comunicación al margen de la función docente universitaria, salvo que la normativa interna de la Universidad lo califique como herramienta profesional al servicio de la institución. De su contenido será responsable el profesor, que deberá observar la normativa de protección de datos en cuanto que incluya información de carácter personal. Por tanto, salvo que se contase con el previo consentimiento de los estudiantes, no se podrían publicar en el blog de un profesor las calificaciones de sus estudiantes.

3.8. HUELLA DIGITAL Y RECONOCIMIENTO FACIAL EN EL ÁMBITO LABORAL

La jurisprudencia del Tribunal Supremo se ha pronunciado sobre el uso de la biometría en el ámbito laboral, afirmando que “[...] Desde luego, la finalidad perseguida mediante su utilización es plenamente legítima: el control del cumplimiento del horario de trabajo al que vienen obligados los empleados públicos. Y, en tanto esa obligación es inherente a la relación que une a estos con la Administración [...], no es necesario obtener previamente su consentimiento ya que el artículo 6.2 de la Ley Orgánica 15/1999 lo excluye en estos casos. Además, no parece que la toma, en las condiciones expuestas, de una imagen de

⁷ El Tribunal Europeo de Derechos Humanos (en adelante, TEDH), en su Sentencia de 5 de septiembre de 2017, as. *Barbulescu v. Rumanía*, considera que existe violación del secreto de las comunicaciones en el despido del demandante por la utilización de mensajería instantánea para uso personal en el centro de trabajo al no ser informado sobre la naturaleza y alcance de la vigilancia a la que iba a ser sometido así como del grado de intrusión en su vida privada y correspondencia.

la mano incumpla las exigencias de su artículo 4.1. Por el contrario, puede considerarse adecuada, pertinente y no excesiva” (por todas, STS núm. 5200/2007, de 2 de julio; FJ 7) (RJ 2007/6598).

No obstante, para que la implantación de un sistema de control horario basado en la recogida de este tipo de datos pueda considerarse proporcionada y, por lo tanto, conforme con el principio de minimización, hay que hacer una evaluación del impacto sobre la protección de datos a la vista de las circunstancias concretas en las que se lleve a cabo el tratamiento para determinar su legitimidad y proporcionalidad, incluido el análisis de la existencia de alternativas menos intrusivas, y establecer las garantías adecuadas. Dándose estas circunstancias, la base legitimadora -si se trata de garantizar el control de cumplimiento del horario- sería el art. 9.2.b) en relación con el art. 6.1.c) RGPD.

Como indica la APDCat, en el caso del control de acceso a dependencias o zonas que requieran unas condiciones de seguridad reforzadas, el uso de este tipo de sistemas puede resultar justificado en determinados casos, si bien también resulta necesario llevar a cabo con carácter previo la evaluación del impacto en la protección de datos (dictamen CNS 63/2018).

En cualquier caso, en lo que respecta a la huella dactilar, se recomienda que superado el juicio de proporcionalidad se instalen preferentemente aquellos sistemas de reconocimiento que permitan que los medios de verificación (algoritmo de la huella dactilar del trabajador), permanezcan en poder de los afectados, sin ser incorporados al sistema, que incluiría los datos identificativos del trabajador al producirse una verificación positiva del mismo, tal y como se recuerda por la Agencia Vasca de Protección de Datos (en adelante, AVPD) (dictamen CN 16-029). En términos análogos se pronuncia la AEPD (informe 0065/2015).

3.9. SISTEMAS BIOMÉTRICOS DE IDENTIFICACIÓN DE LA PERSONA PARA FINES NO LABORALES

El control de acceso de las personas a las instalaciones estaría legitimado en el art. 6.1.e) RGPD (garantía de la seguridad de las personas, bienes e instalaciones). Sin embargo, hay que analizar si el uso de sistemas biométricos de identificación de las personas para estos fines (por ejemplo, para preservar la seguridad de acceso a las bibliotecas universitarias, asistencia a clase, acceso a comedores, entre otros) es adecuado, pertinente y limitado a lo necesario en relación a estos. En otras palabras, habría que determinar si no hay medios menos intrusivos en la intimidad de las personas, como indica la AEPD, a la vista de la evaluación de impacto que se realice (informe 0065/2015).

Por ejemplo, no sería acorde con los principios contemplados en el art. 5 RGPD el tratamiento de los datos de reconocimiento facial de los estudiantes de los centros universitarios para el control de su asistencia a las clases y de su efectiva participación en las pruebas que se desarrollen en el centro, tal y como pone de manifiesto la AEPD (informe 0392/2011).

4. IMÁGENES

4.1. TRATAMIENTO DE IMÁGENES POR RAZONES DE SEGURIDAD

- *Indicaciones sobre zonas de grabación de imágenes por razones de seguridad*

Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones. En ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado.

La zona objeto de videovigilancia será la mínima imprescindible abarcando espacios públicos como accesos o pasillos.

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

No podrán utilizarse con fines de control de asistencia a clase, al existir otros medios menos intrusivos o invasivos de la intimidad.

- *Las cámaras de seguridad no graban las imágenes limitándose a su reproducción en tiempo real*

Las previsiones contenidas en el RGPD y en la LOPDGDD resultan de aplicación a la captación de imágenes, con independencia de que éstas se graben o no.

- *Cesión de imágenes a las fuerzas y cuerpos de seguridad*

Son de aplicación las mismas observaciones que se han especificado en el epígrafe de “estudiantes”. En cualquier caso, las solicitudes de grabaciones en los supuestos descritos debe realizarse de forma motivada en cada caso concreto, y la entrega de las mismas debe ser proporcional a la finalidad del requerimiento realizado, sin que se produzca una comunicación indiscriminada.

- *Cesión de imágenes de un accidente producido en las instalaciones de la Universidad a compañía aseguradora*

La cesión de las imágenes en las que se constata el accidente sufrido en las instalaciones universitarias, se efectúa a la compañía de seguros con la que la institución tenga contratado el correspondiente seguro. Esta comunicación tiene su base legitimadora en el artículo 6.1.c) RGPD, al existir una norma con rango de ley (Ley 50/1980, de Contrato de Seguro), de la que se deriva la obligación del asegurado de facilitar al asegurador toda la información relacionada con las circunstancias del siniestro (informe AEPD 0020/2014).

- *Cesión a particulares de imágenes grabadas en el parking de las instalaciones universitarias*

Se puede ceder los datos de las imágenes obtenidas por las videocámaras instaladas en el aparcamiento a fin de obtener una prueba de la relación de causalidad de daños en el vehículo de un usuario por otro usuario del aparcamiento, siempre que la finalidad de la comunicación de datos no sea otra que la de su presentación en juicio. En este caso, habría interés legítimo -art. 6.1.f) RGPD- ya que los derechos a la tutela judicial efectiva y a la defensa de la persona prevalecerían sobre el



derecho a la protección de datos del afectado, siempre que, atendiendo al principio de minimización, se comuniquen solo aquellas imágenes limitadas al incidente, de manera que no se aporten datos de otras personas (ya sean imágenes de las mismas o matrículas de vehículos) que no tengan que ver con el mismo (informe AEPD 0115/2012).



Buena práctica: exigir un compromiso por escrito por parte del solicitante de que la única finalidad del uso de los datos personales comunicados será la descrita anteriormente, advirtiéndole de las responsabilidades en materia de protección de datos que pueden asumirse en caso de cualquier otro uso de dichos datos.

4.2. TRATAMIENTO DE IMÁGENES CON FINES EDUCATIVOS, INSTITUCIONALES O CULTURALES

- *Elaboración de videotutoriales por los estudiantes y posterior publicación en el blog de la Universidad*

La elaboración y ulterior publicación de los videotutoriales se ha de fundamentar en el previo consentimiento otorgado por los estudiantes o personas que aparezcan en los videos, salvo que se trate de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público (art. 8.2.a Ley Orgánica 1/1982, de 5 de mayo, de protección civil de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, en adelante LO 1/1982).

- *Exposición o stand con fotos captadas en actos y eventos de la universidad*

La divulgación de las fotos (si en ellas aparecen datos personales) es una comunicación de datos, para la que sería necesario el previo consentimiento de las personas fotografiadas, salvo que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público (art. 8.2.a LO 1/1982).

Utilización de imágenes de los miembros de la comunidad universitaria o de terceras personas en acciones promocionales de la Universidad, en memorias, guías, revistas, proyectos de innovación docente con fines de difusión de la metodología en entornos académicos o científicos externos, entre otros.

Para la divulgación de las imágenes se requiere el previo consentimiento de los afectados, salvo que resulte de aplicación cualquier otra base de legitimación.

- *Publicación de fotos de antiguos alumnos de una determinada promoción*

Se requiere el previo consentimiento de los afectados, salvo que resulte de aplicación cualquier otra base de legitimación.

- *Grabación de la sesión de una clase en video*

En el supuesto de que sea el estudiante el que pretende la grabación será necesario el previo consentimiento de los afectados, incluido el profesor.

Si es el profesor el que está interesado en la grabación será posible, sin previo consentimiento de los asistentes a la clase, si se trata de una grabación que efectúe el docente exclusivamente en el ejercicio de la función educativa en cuyo caso sería de aplicación el artículo 6.1.e) RGPD (tendría su legitimidad

legal en la actividad y formación docente prevista en la Ley Orgánica de Universidades), y sin ulterior utilización para otros fines (entre ellas, su divulgación). Las imágenes solo deberán estar accesibles para los estudiantes participantes en dicha actividad y el profesor correspondiente. Si la citada grabación pudiera afectar al derecho al honor, a la imagen o a la intimidad personal de cualquiera de los asistentes, se requeriría su previo consentimiento.



Buena práctica: divulgar a través de las listas institucionales los requisitos para poder proceder a la grabación sin consentimiento expreso y de las responsabilidades en materia de protección de datos que pueden asumirse en caso de incumplimiento, o colocar paneles o carteles informativos en la entrada de las aulas explicando dichos requisitos.

- *Grabación de las imágenes de los alumnos durante la realización de los exámenes*

Con carácter general, no sería una medida proporcionada y adecuada para la finalidad perseguida, pudiéndose valorarse otros medios menos intrusivos para la privacidad de las personas si la finalidad es disuadir a los estudiantes de determinadas conductas durante la realización de los exámenes o hacer un mejor y adecuado seguimiento de su evaluación.

En su [informe 0186/2017](#), la AEPD recuerda que las aulas son un espacio semi privado, en sentido técnico jurídico, y la citada grabación pudiera constituir una intromisión ilegítima en los términos previstos en la LO 1/1982.

Por ello, para la autoridad de control, la instalación de cámaras en las aulas con la finalidad de disuadir a los alumnos de cometer determinadas conductas inapropiadas durante la celebración de los exámenes sólo podría considerarse bajo determinadas circunstancias (cuando exista un bien jurídico superior concreto que lo justifique, y con su correspondiente base legitimadora) y con especiales salvaguardas, pero no como una medida a implementar con carácter general en la Universidad ([informe 0186/2017](#)).

- *Uso de imágenes realizadas en actividades académicas, culturales, deportivas, entre otras, correspondientes a actos organizados por la Universidad y su posterior difusión en el canal de noticias de la página web de la Universidad o en las redes sociales institucionales*

El hecho de que la realización de las fotos o la grabación de los videos se produzcan durante un acto público no legitima para excluir el previo consentimiento inequívoco de las personas grabadas o fotografiadas, salvo que:

1. Se trate exclusivamente de captar la imagen de los asistentes de forma accesoria y sin posterior divulgación, o
2. Se tomen en un acto de interés histórico, científico o cultural relevante (art. 8.1 de la LO 1/1982).

En lo que respecta al carácter accesorio de las imágenes, hay que tener en cuenta que en estos casos, estrechamente vinculado con el derecho de protección de datos, está el derecho a la propia imagen, que ha sido definido por la jurisprudencia como un derecho que tiene “*cada individuo a que los demás no reproduzcan los caracteres esenciales de su figura sin el consentimiento del sujeto, de tal manera que todo acto de captación, reproducción o publicación por fotografía, film u otro procedimiento de la imagen de una persona en momentos de su vida privada o fuera de ella supone una vulneración o ataque al derecho fundamental a la imagen, como también lo es la utilización para fines publicitarios, comerciales o de naturaleza análoga*” (STS núm. 256/1999, de 27 de marzo; FJ 3) (RJ 1999/2370).

A la vista de esta doctrina, no sería preciso el consentimiento de los afectados en aquellos supuestos en que su imagen sea captada en relación con un suceso o acontecimiento público y aparezca como meramente accesorio. En ese sentido se han pronunciado la AVPD en su [dictamen CN 18-005](#) y la APDCat en su [dictamen CNS 64/2015](#).

Respecto al carácter accesorio de las imágenes, el artículo 8.2 c) de la LO 1/1982 establece que el derecho a la propia imagen no impedirá *“la información gráfica sobre un suceso o acaecimiento público cuando la imagen de una persona determinada aparezca como meramente accesorio”*. Por su parte, el Alto Tribunal en su [STS núm. 220/2014, de 7 de mayo](#), afirma que *“hay abundante doctrina de esta Sala que toma en cuenta el carácter accesorio de la imagen de una persona, respecto del texto escrito o el contexto de la fotografía o fotograma y que declara que existe tal carácter cuando la imagen no es elemento principal, porque no es necesaria la presencia, ni tiene especial relación con el objeto de la captación o proyección, y no hay nada desmerecedor o de desdoro para el afectado, esta doctrina está ligada siempre a un acontecimiento público”* (FJ 10) (RJ 2014/3299).

El Tribunal Supremo vincula pues el carácter accesorio de una imagen cuando no es necesaria su presencia, estando la intromisión justificada en la medida en que la imagen es captada de manera accidental y secundaria en relación con el resto de la información en la que inserta. En su [sentencia núm. 196/2007](#), de 22 de febrero, el Alto Tribunal se refiere al supuesto de una grabación en video (RJ 2007/1518).

Por consiguiente, concurriendo las circunstancias expuestas, la base legitimadora de la captación de las imágenes por parte de la Universidad en eventos públicos que organice sería el artículo 6.1.e) RGPD. En caso de no estar ante una imagen meramente accesorio o accidental sería necesario el previo consentimiento de los afectados.

Por su parte, se podrá difundir las imágenes captadas en actos académicos relevantes (entre otros, concesión de honoris causa, inauguración del curso académico), cuando afecten a personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública, puesto que se estaría ante un interés público -art. 6.1.e) RGPD- con amparo en el art. 8.2.a) de la LO 1/1982.

En los restantes supuestos, se requiere el consentimiento inequívoco de las personas que aparezcan en las imágenes que se van a divulgar para su posterior difusión pública. En el caso de los menores de catorce años, dicho consentimiento deberá ser otorgado por el titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela (art. 7.2 LOPDGDD).



Buena práctica:

- Informar a la entrada del evento de la finalidad de la grabación de imágenes de los asistentes (mediante carteles o paneles informativos, folletos, entre otros).
- Si se cursa invitación se debe advertir de que la Universidad tomará fotografías y/o grabará vídeos.
- Los fotógrafos oficiales deberían de llevar una acreditación que los distinga como tales. Si la captación y uso de imágenes va a ser particularmente intensiva se recomienda repartir algún tipo de distintivo (chapa, pegatina, entre otros) de color entre los asistentes que permita a los fotógrafos evitar a aquellos que no desean ser retratados.
- Los fotógrafos oficiales centrarían la captura de imágenes y vídeos del evento en tomas generales de los asistentes, de forma que ninguno adquiera un papel exclusivo o predominante y la presencia de cualquiera de ellos pueda entenderse como accesorio.

- *Grabación de imágenes y toma de fotografías en un acto universitario por parte de particulares*

Las grabaciones y toma de fotografías de las imágenes de familiares que participan en eventos universitarios se encontrarían amparadas en el ámbito personal y doméstico y, por tanto, excluido de la aplicación del RGPD (art. 2.2.c) en la medida en que las imágenes sean tomadas por particulares para sus fines familiares. En todo caso, el uso social permite este tipo de grabaciones y realización de fotografías.

Asimismo, esta excepción, de conformidad con el considerando 18 del RGPD, se aplicaría a la actividad de redes sociales y la actividad en línea siempre y cuando se encuentre vinculada exclusivamente a una actividad personal o doméstica, sin perjuicio de la aplicación de la norma europea a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas. Apunta la [STJUE de 6 de noviembre de 2003](#), as. C-101/01, *Lindqvist*, que “esta excepción debe interpretarse en el sentido de que contempla únicamente las actividades que se inscriben en el marco de la vida privada o familiar de los particulares”.

En este sentido, no podrán entenderse exceptuados aquellos supuestos en los que la información tratada sea puesta en conocimiento de un número indeterminado o indefinido de personas. Por ello, si se graban imágenes o toman fotos de terceras personas y/o se divulguen en redes sociales, páginas web o mediante Whatsapp, se requeriría el previo consentimiento de estas.

Por último, conviene recordar que, aunque el derecho a la protección de datos no resulte de aplicación en los supuestos previstos en el citado art. 2.2.c) RGPD, sí pueden ser aplicable en estos casos otras normas, como las que protegen frente a las intromisiones que supongan una vulneración de los derechos al honor, a la intimidad y a la propia imagen (LO 1/1982), o la legislación de protección del menor.



Buena práctica: informar mediante paneles o carteles informativos a los particulares de su responsabilidad en materia de protección de datos en caso de que las imágenes de terceras personas que hayan grabado fueran divulgadas en entornos abiertos (entre ellas, redes sociales, páginas web) sin contar con el previo consentimiento de las personas afectadas.

- *Grabación de imágenes en instalaciones deportivas de la Universidad*

La captación de imágenes de personas físicas identificadas o identificables que se encuentren en instalaciones universitarias podría ser conforme con la normativa de protección de datos en la medida que las imágenes de estas personas aparezcan como meramente accesorias en eventos públicos, tales como, en un encuentro deportivo, de conformidad con el artículo 8.2.c) de la LO 1/1982.

En particular, se considera que la captación de imágenes de las personas que se entrenan en estas instalaciones no estaría habilitada por la LO 1/1982, dado que los entrenamientos no tendrían consideración “de evento público”, y su grabación claramente conllevaría la captación continua y no accesoría de las imágenes de las personas que los efectúan y que pueden tener al respecto unas justificadas expectativas de privacidad, por lo que requerirían consentimiento expreso de los afectados (o, en su caso, de sus padres, tutores o representantes legales), como apunta la APDCat en su [dictamen CNS 3/2015](#).

4.3. TRATAMIENTO DE IMÁGENES CON FINES DE CONTROL LABORAL

- *Uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo*

Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de video-



vigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales -art. 20 bis del TRLET y art. 14.j) bis del Estatuto Básico del Empleado Público (en adelante, TRLEBEP)-.

De conformidad con lo dispuesto en el artículo 89 de la LOPDGDD, los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del TRLET y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida⁸.

En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos un dispositivo informativo colocado en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 RGPD⁹. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información.

En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.

La utilización de sistemas similares a los referidos anteriormente para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, deberán ser puestos a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

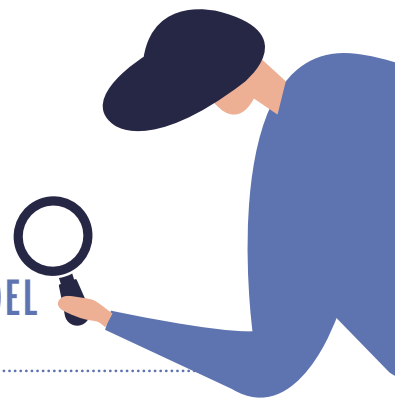
4.4. TRATAMIENTO DE IMÁGENES CON FINES CIENTÍFICOS

- *Captación y grabación de imágenes para fines de investigación científica*

Se requerirá el previo consentimiento del afectado, salvo que resulte de aplicación cualquier otra base de legitimación. Hay que recordar que el tratamiento de datos personales como las imágenes con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, estará sujeto a las garantías adecuadas para los derechos y libertades de los interesados, disponiendo de medidas técnicas y organizativas, en particular para garantizar el principio de minimización de los datos personales, pudiendo incluir la "seudonimización", siempre que de esa forma puedan alcanzarse dichos fines (art. 89 RGPD).

⁸ El legislador, en este sentido, ha venido a dar carta de naturaleza legal a la doctrina del intérprete constitucional en la materia. Por todas, STC núm. 29/2013, de 11 de febrero (RTC 2013\29) y STC núm. 39/2016, de 3 de marzo (RTC 2016\39). Véase asimismo la STEDH de 9 de enero de 2018, as. *López Ribalda y otros v. España*, que incide en excluir expresamente la licitud de las grabaciones encubiertas o no informadas e impone el carácter absoluto del deber informativo.

⁹ En este sentido, la SJSO de Pamplona núm. 281/2019, de 18 de febrero (AS 2019\1014) extiende el deber informativo sobre la existencia de sistema de videovigilancia y la propia finalidad para la que se utilizaba a la posibilidad de sancionar si captan actos ilícitos o incumplimientos laborales (FJ 2).



5. ACTIVIDAD INVESTIGADORA Y DE TRANSFERENCIA DEL CONOCIMIENTO

5.1. PUBLICIDAD ACTIVA¹⁰

- Producción y divulgación científica; proyectos de investigación, según “ranking”
- Grupos de investigación: catálogo, número de miembros y colaboradores, proyectos asociados, fuentes de financiación
- Proyectos nacionales, europeos e internacionales
- Centros y servicios de investigación (institutos, laboratorios, etc.)
- Principales resultados relacionados con la actividad investigadora: sexenios, tesis defendidas, ponencias, comunicaciones, índices de impacto, “ranking” de investigadores, presencia de la Universidad en los “ranking” de calidad científica, en redes sociales, etc.)
- Principales resultados relacionados con la transferencia de los resultados de investigación: publicaciones, patentes solicitadas y concedidas, creación de empresas de base tecnológica
- Plan propio de investigación: programas de I+D+i, ayudas para la realización de tesis doctorales, bolsas de viaje, organización de congresos y conferencias
- Datos agregados sobre recursos humanos: personal investigador en formación, contratos con cargo a proyectos, otros contratos, etc
- Internacionalización: proyectos compartidos, indicadores de movilidad internacional en centros de investigación, financiación obtenida
- Estancias del personal investigador en centros de investigación nacionales e internacionales.
- Cátedras institucionales y de empresa
- Comisiones I + D + i (comités de ética, normas, etc.)
- Memorias de investigación
- Evolución del número de doctores participantes en contratos y convenios
- Actuaciones en infraestructuras científico-tecnológicas
- Resultados obtenidos por los grupos de investigación de la Universidad en evaluaciones efectuadas por la Agencia Estatal de Investigación (AEI), por otras instituciones, organizaciones o la propia Universidad
- Ayudas, premios, incentivos y reconocimientos a la excelencia académica, investigadora y docente que se otorgan en la Universidad
- Tesis doctorales (datos de referencia, índices de impacto, etc.)

5.2. REALIZACIÓN DE ESTUDIOS

- *Acceso a datos de archivos históricos universitarios para estudios científicos*

En principio, habría que analizar si, en función de la finalidad investigadora que se pretende, puede facilitarse la información disociada o anonimizada.

¹⁰ Véase la nota a pie 1 de la presente guía.

Si no fuera posible, habría que atender a las siguientes reglas:

- a. En cuanto a los datos personales que no tengan la consideración de especialmente protegidos habría que realizar el test del daño, así como la ponderación prevista en el art. 15.3 de la LTAIBG. Entre otros criterios a tener en cuenta estarían, por ejemplo, el transcurso de los plazos establecidos en el artículo 57.1.c) de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español (en adelante, LPHE) (veinticinco años desde el fallecimiento de su titular, si la fecha es conocida o, en otro caso, de cincuenta años, a partir de la fecha de los documentos), así como la justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos.
- b. En cuanto a los datos especialmente protegidos contenidos en la documentación solicitada hay dos líneas interpretativas, en función de la exégesis de la expresión “o, en otro caso” contenida en el meritado art. 57.1.c) LPHE:
 - i. La que abogaría por considerar que los cincuenta años desde la fecha del documento ha de interpretarse en el sentido de desconocer la fecha del óbito pero sí el hecho del fallecimiento. Esta postura es avalada por la APDCat ([informe IAI 20/2016](#)), la Comisión de Garantía del Derecho de Acceso a la Información Pública (en adelante, GAIP) ([R 69/2016](#)), y por la más reciente doctrina de la AVPD ([dictamen CN 14-024](#)). Esta línea incide en la garantía que supone no comunicar información íntima relativa a personas vivas, aunque mantiene disenso en cuanto a quién debería acreditar el fallecimiento (si la Administración o el propio solicitante).
 - ii. La que postula la consulta de los documentos que obren en archivos históricos, siempre que hayan transcurrido cincuenta años desde la fecha de los documentos, si no consta si el afectado ha fallecido o no. Esta postura es defendida por la AEPD en diversos informes (por todos, [0120/2010](#); [0243/2010](#)).

En esta guía se aboga por la interpretación realizada por la AEPD, si bien puntualizando que el simple hecho de que hayan transcurrido los cincuenta años no es una habilitación general para el acceso a la citada documentación, sino que habrá que ponderar en cada caso concreto si existe causa de legitimación suficiente para el acceso. En este sentido, el art. 28.2 del Real Decreto 1708/2011 pone de relieve que *“Cuando no fuera posible conocer la fecha o el hecho del fallecimiento y el documento o documentos solicitados posean una antigüedad superior a cincuenta años, el acceso se concederá si, atendidas las circunstancias del caso, se entiende razonablemente excluida la posibilidad de lesión del derecho a la intimidad personal y familiar o el riesgo para la seguridad del afectado y siempre de conformidad con la normativa de protección de datos”*.

Conviene recordar también que existe un amplio plazo para ejercitar las acciones civiles de protección de los derechos fundamentales al honor, a la intimidad personal y familiar y a la propia imagen (art. cuarto Ley Orgánica 1/1982), por lo que el tratamiento de los datos personales a los que se refiere el citado art. 57.1.c) de la LPHE ha de respetar el ámbito de intimidad personal, familiar, la imagen y el honor del afectado.

En síntesis, cuando se pretenda el acceso a datos especialmente protegidos de personas vivas habrá que recabar el previo consentimiento de estas. Si han fallecido tendrá que haber transcurrido el plazo de veinticinco años desde su muerte, si se conoce la fecha del óbito. Por último, habrá que atender al transcurso del plazo de cincuenta años si no consta si el afectado falleció o no, con las prevenciones indicadas anteriormente, todo ello salvo que la legislación autonómica aplicable disponga lo contrario¹¹.

¹¹ Véase asimismo el art. 26 de la LOPDGDD.

- *Un investigador solicita acceder a datos de contacto del personal docente o de estudiantes para realizar una encuesta*

Si la investigación se efectúa a nivel institucional (en el marco de un proyecto de investigación concreto), se podrá facilitar los correos de contacto (en el caso del profesorado su cuenta profesional, y en el de los estudiantes el correo que la Universidad le asigne) con fundamento en el interés público -art. 6.1.e) RGPD- el desarrollo de la investigación científica, técnica y artística y la transferencia del conocimiento.



Buena práctica: habilitar una lista de distribución específica y temporal para esta finalidad.

En cualquier caso, debería de insertarse en el cuestionario un enlace a la política de privacidad que regule el tratamiento de datos derivados de encuestas.

En el caso de tratarse de un estudio o investigación que se realice a título personal habría que realizar el test del daño, así como el juicio de ponderación previsto en el art. 15.3 de la LTAIBG, para determinar, en función de las circunstancias concurrentes en cada supuesto, si se acredita un interés legítimo y, en su caso, si este prevalece sobre el derecho a la protección de datos.

- *Cesión de datos de estudiantes y profesorado para realización del TFM/TFG o la Tesis Doctoral*

Se trata de estudio o investigación que se realiza a título personal, por lo que habría que realizar el test del daño, así como el juicio de ponderación previsto en el art. 15.3 de la LTAIBG, para determinar, en función de las circunstancias concurrentes en cada supuesto, si existe un interés legítimo y, en su caso, si este prevalece sobre el derecho a la protección de datos. En el caso de acceso a datos personales contenidos en archivos históricos universitarios habría que atender a lo indicado en este punto *ut supra*.

La solicitud se inadmitiría a trámite si supone para la Universidad la elaboración no de un documento sino de múltiples documentos expresos, debiendo acudir a distintas fuentes de información, siempre que carezcan de los medios técnicos que permitan recopilar toda la información solicitada sin tener que acudir a una búsqueda manual que no sea proporcionada -art. 18.1.c) LTAIBG o, en su caso, precepto equivalente del resto de leyes autonómicas de transparencia¹².

- *Cesión de datos a catedrático jubilado para realización de estudio*

Se trata de estudio o investigación que se realiza a título personal, por lo que habría que realizar el test del daño, así como el juicio de ponderación previsto en el art. 15.3 LTAIBG, para determinar, en función de las circunstancias concurrentes en cada supuesto, si existe un interés legítimo y, en su caso, si este prevalece sobre el derecho a la protección de datos. En el caso de acceso a datos personales contenidos en archivos históricos universitarios habría que atender a lo indicado en este punto *ut supra*.

- *Cesión de datos entre administraciones para estudios científicos*

Si se trata de un estudio incardinado en un proyecto institucional su título legitimador sería el art. 6.1.e) RGPD, sin que sea necesario, por consiguiente, con carácter general, el consentimiento del titular de

¹² Puede consultarse el criterio interpretativo del CTBG (007/2015), de 12 de noviembre de 2015, relativo a las causas de inadmisión de solicitudes de información: relativas a información para cuya divulgación sea necesaria una acción previa de reelaboración, a través del enlace al citado órgano que consta en el [Anexo III](#) de la presente guía. Asimismo, el CTBG se ha pronunciado sobre la acción previa de reelaboración en diversas resoluciones, que incluyen jurisprudencia en la materia. Por todas, [RT/0496/2018](#); [R/0280/2018](#); [R/0117/2016](#)).

los datos, dado que se produce entre Administraciones públicas y tiene como objeto su tratamiento posterior con finalidad de carácter científico (por todos, [informe AEPD 9901/2002](#)).

En cualquier caso, para el tratamiento de datos personales con fines históricos, científicos o estadísticos se ha de estar a las siguientes reglas:

- a. Los datos personales han de limitarse a los estrictamente necesarios y limitados a la finalidad científica concreta que se persigue.
- b. Se han de ofrecer las garantías previstas en el artículo 89 RGPD (“seudonimización”, cifrado, etc.).
- c. Los miembros del grupo de investigación deberán respetar el deber de confidencialidad que establece el artículo 5.1 de la LOPDGDD.
- d. La finalización del estudio debe comportar necesariamente la eliminación de los datos personales de las personas interesadas.

No obstante, como indica la AEPD, si la comunicación contiene datos especialmente protegidos (como, por ejemplo, datos de salud) se ha de solicitar el previo consentimiento expreso del interesado, con independencia de que el trabajo a desarrollar se inserte o no en el marco de un proyecto institucional ([informe 0317/2009](#)).

Sin embargo, señala la AEPD que si lo que se pretende con la comunicación es el tratamiento ulterior de los datos personales con fines estadísticos, el estudio tendría que ser considerado como estadística de cumplimentación obligatoria a los efectos previstos en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, o legislación autonómica correspondiente¹³. En caso contrario, se necesitaría el previo consentimiento de los afectados ([informe 0379/2009](#)).

- *Estudio de inserción laboral y estudio de egresados por la Universidad*

Si el estudio lo realiza un órgano universitario en el ejercicio de sus funciones o investigadores de la propia Universidad a nivel institucional, la comunicación de datos personales encontraría habilitación suficiente al amparo del artículo 6.1.e) RGPD. En cualquier caso, los datos personales han de limitarse a los estrictamente necesarios y limitados a la finalidad científica concreta que se persigue.

- *Tratamiento de datos en la investigación en salud*

El legislador ha considerado incluidos en los supuestos de las letras g), h), i) y j) del artículo 9.2 RGPD a los tratamientos de datos relacionados con la salud regulados en la normativa de salud pública, pero estableciendo unas consideraciones específicas respecto de los estudios científicos que puedan llevarse a cabo con dichos datos de salud, para los cuales no será necesario contar con el consentimiento de las personas afectadas, cuando se trate de situaciones de excepcional relevancia y gravedad para la salud pública, no por tanto cuando no se den estas circunstancias –apartado 2.b) de la disposición adicional decimoséptima LOPDGDD–.

Por ello, no dándose los supuestos previstos anteriormente, será necesario el consentimiento del interesado o, en su caso, de su representante legal para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora.

Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad con-

¹³ Véase asimismo el dictamen CNS 49/2018 de la APDCat.

creta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial.

En los casos indicados en el párrafo anterior, los responsables deberán publicar la información establecida por el artículo 13 RGPD en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato.

Para los tratamientos de reutilización de datos personales con fines de investigación en materia de salud y biomédica, se requerirá informe previo favorable del comité de ética de la investigación.

Se considera lícito el uso de datos personales “seudonimizados” con fines de investigación en salud y, en particular, biomédica.

El uso de datos personales “seudonimizados” con fines de investigación en salud pública y biomédica requerirá:

- a.** El informe previo del comité de ética de la investigación previsto en la normativa sectorial. En defecto de la existencia del mencionado Comité, la entidad responsable de la investigación requerirá informe previo del delegado de protección de datos.
- b.** Una separación técnica y funcional entre el equipo investigador y quienes realicen la “seudonimización” y conserven la información que posibilite la reidentificación.
- c.** Que los datos “seudonimizados” únicamente sean accesibles al equipo de investigación cuando:
 - i.** Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.
 - ii.** Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.

Podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos “seudonimizados”, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria.

Cuando se traten datos personales con fines de investigación en salud, y en particular la biomédica, a los efectos del artículo 89.2 RGPD, podrán excepcionarse los derechos de los afectados previstos en los artículos 15, 16, 18 y 21 RGPD cuando:

- a.** Los citados derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o “seudonimizados”.
- b.** El ejercicio de tales derechos se refiera a los resultados de la investigación.
- c.** La investigación tenga por objeto un interés público esencial relacionado con la seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley.

Por último, cuando conforme a lo previsto por el artículo 89 RGPD, se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a:

- a. Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del RGPD o en los establecidos por la autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la “anonimización” o “seudonimización” de los datos.
- b. Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica.
- c. Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.
- d. Designar un representante legal establecido en la Unión Europea, conforme al artículo 74 RGPD, si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 RGPD.

5.3. ACCESO A MATERIAL CIENTÍFICO

- *Acceso a la producción científica de un investigador*

Según dispone el art. 37.1 de la Ley 14/2011, de la Ciencia, la Tecnología y la Innovación, los agentes públicos del Sistema Español de Ciencia, Tecnología e Innovación [entre los que se encuentran las universidades públicas] impulsarán el desarrollo de repositorios, propios o compartidos, de acceso abierto a las publicaciones de su personal de investigación, y establecerán sistemas que permitan conectarlos con iniciativas similares de ámbito nacional e internacional.

La versión electrónica se hará pública en repositorios de acceso abierto reconocidos en el campo de conocimiento en el que se ha desarrollado la investigación, o en repositorios institucionales de acceso abierto.

Sin embargo, no se ha dado aún cumplimiento a lo dispuesto en la disposición adicional novena de la citada norma legal, en virtud de la cual “*el Gobierno regulará, previo informe de la Agencia Española de Protección de Datos, el contenido académico y científico de los currículos del personal docente e investigador de Universidades y del personal investigador que los agentes de financiación y de ejecución pueden hacer público sin el consentimiento previo de dicho personal*”, ni tampoco al mandato establecido en el apartado 5 de la disposición adicional vigesimoprimeras de la Ley Orgánica 4/2007, de 12 de abril, que modifica la LOU.

A la vista de esta regulación, en conexión con la transparencia pública, afirma la APDCat que:

“[...] la legislación general de transparencia también puede comportar que se deba dar difusión a determinada información sobre la organización, la gestión y la actividad de las universidades, en concreto, a los efectos que interesan, información sobre la actividad docente e investigadora que llevan a cabo.

Todo ello, sin perjuicio de que habrá que respetar, si procede, las limitaciones que puedan derivarse de otra normativa, como podría ser, entre otras, la legislación de propiedad intelectual (Real Decreto Legislativo 1/1996, de 12 de abril, que aprueba el Texto refundido de la Ley de propiedad intelectual), respecto a la difusión de información relativa a trabajos de investigación o tesis doctorales de los investigadores afectados.

Por todo lo expuesto, a los efectos del principio de licitud (art. 6.1 RGPD), y a la vista de la normativa estudiada, habría que considerar que las diferentes universidades sometidas a las previsiones de dicha normativa, como responsables del tratamiento en los términos apuntados, pueden estar habilitadas para dar difusión en abierto, tanto a través de sus propios sitios web o canales de información [...], de determinada información profesional sobre sus investigadores y sobre las publicaciones y la actividad docente e investigadora de estos; para concluir que “[...] No parece que se pueda dar cumplimiento adecuado a la finalidad de transparencia y calidad de las universidades prevista en la normativa en los términos apuntados sin difundir información sobre la producción científica y la investigación en el ámbito universitario, asociada a sus autores (los investigadores, en este caso)”.

Por ello, considera la citada autoridad de control que es adecuada la difusión de las publicaciones, presentación de trabajos en congresos, documentos científico-técnicos; participaciones en proyectos R+D+i y competitivos y tesis doctorales (leídas o dirigidas) sobre la producción y publicación de los investigadores ([dictamen CNS 53/2018](#)).

Todo lo expuesto anteriormente se entiende sin perjuicio de los acuerdos en virtud de los cuales se hayan podido atribuir o transferir a terceros los derechos sobre las publicaciones, y no será de aplicación cuando los derechos sobre los resultados de la actividad de investigación, desarrollo e innovación sean susceptibles de protección.

En una interpretación acorde con el derecho a la propiedad intelectual del propio autor, parece razonable que los fines de transparencia de la producción científica y su proyección se satisfagan con la publicación de la relación de los resultados de esa actividad (relaciones de publicaciones, participaciones en congresos, proyectos, tesis dirigidas, etc.), requiriéndose para el acceso al contenido del material científico del previo consentimiento de su autor/es, siempre que no exista un interés legítimo debidamente acreditado.

También debe tenerse en cuenta que las tesis doctorales, en virtud de lo previsto en la legislación vigente, se archivan en formato electrónico abierto en el repositorio institucional, por lo que pueden ser consultadas libremente, salvo en circunstancias excepcionales determinadas por la comisión académica del programa, como pueden ser, entre otras, la participación de empresas en el programa o Escuela, la existencia de convenios de confidencialidad con empresas o la posibilidad de generación de patentes que recaigan sobre el contenido de la tesis.

La AEPD se ha pronunciado en contra de la cancelación dado que la publicación en internet de la tesis a través del repositorio de la Universidad está regulada en el art. 14.5 RD 99/2011 ([TD-00137/2015](#)). Por su parte, el Consejo de Transparencia, Acceso a la Información Pública y Buen Gobierno de la Comunidad Valenciana, considera que tratándose de trabajos divulgados con consentimiento del autor debe prevalecer el derecho de acceso, teniendo en cuenta que no se ven cuestionados los derechos derivados de la propiedad intelectual ([R 3/2016](#)).

Por su parte, la Ley 14/2011 dispone que *“el personal de investigación cuya actividad investigadora esté financiada mayoritariamente con fondos de los Presupuestos Generales del Estado hará pública una versión digital de la versión final de los contenidos que le hayan sido aceptados para publicación en publicaciones de investigación seriadas o periódicas, tan pronto como resulte posible, pero no más tarde de doce meses después de la fecha oficial de publicación”.*

En cualquiera de los supuestos indicados en los que proceda el acceso, será de aplicación ulterior la legislación en materia de propiedad intelectual (art. 4 Real Decreto Legislativo 1/1996).

5.4. DIFUSIÓN DE NOTICIAS

- *Difusión a través del correo electrónico profesional del personal investigador de convocatorias y boletín informativo de la actividad investigadora*

El tratamiento se considera lícito al ser necesario en el contexto de la relación contractual, por lo que no sería necesario el consentimiento-art. 6.1.b) RGPD-.



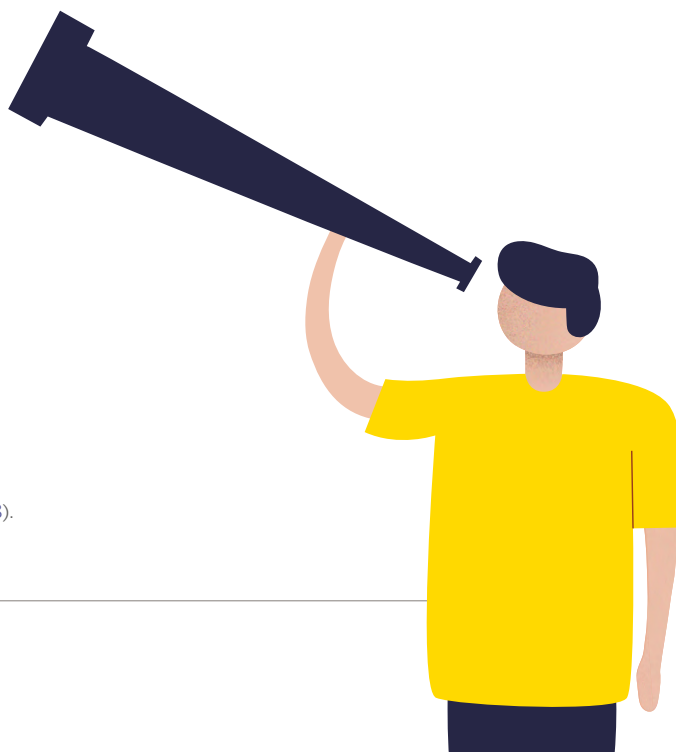
Buena práctica: se recomienda la utilización de listas de distribución para estos supuestos.

5.5. ACCESO A INFORMACIÓN RELATIVA A PROYECTOS DE INVESTIGACIÓN

Como señala la APDCat, en una interpretación conjunta de la LOU y la Ley 14/2011 (legislación sectorial) y la legislación de transparencia, existe habilitación legal para que difundir determinada información sobre la evaluación de la actividad docente e investigadora, en términos de publicidad activa, entre ella la relación de los proyectos de investigación que se han llevado a cabo en la Universidad, con identificación de las personas que han participado, entre ellos el de la persona que consta como investigador principal.

Tampoco impediría que al solicitante del derecho de acceso a la información pública se le facilitasen los informes de seguimiento de proyectos y la justificación de gastos, incluidas las facturas solicitadas, así como la información sobre la contratación, incluyendo la identidad de las personas afectadas, salvo que concurran circunstancias especiales en cada caso. Todo ello, sin perjuicio de omitir aquellos datos identificativos (como el NIF o el domicilio de las personas afectadas) así como otros datos personales que, más allá de la identificación del adjudicatario o de los docentes e investigadores asignados a los proyectos, puedan constar en la documentación solicitada y sean innecesarias para alcanzar la finalidad de transparencia perseguida ([informe IAI 12/2019](#))¹⁴.

Todo lo expuesto anteriormente se entiende salvo que existan motivos razonados para preservar la actividad de investigación, desarrollo e innovación, por su específica naturaleza que la haga susceptible de sujeción a alguno de los límites del art. 14 LTAIBG (cláusulas de secreto profesional, propiedad intelectual e industrial, etc.)¹⁵.



¹⁴ La GAIP asume este criterio ([resolución 259/2018](#)).

¹⁵ Por todas, R/0206/2016 del CTBG.



6. INFORMACIÓN ECONÓMICO-FINANCIERA

6.1. PUBLICIDAD ACTIVA¹⁶

Entre otro tipo de información, se recomienda hacer pública la siguiente:

- Informes internos y externos de auditoría de cuentas
- Indicadores de control presupuestario: modificaciones, grado de ejecución (por trimestres) y cumplimiento, ejercicios cerrados
- Indicadores financieros: liquidez inmediata o de disponibilidad, liquidez general, grado de solvencia, deuda acumulada e índices de autonomía o independencia financiera
- Indicadores de gestión económica: datos de facturación y promedios de abono a proveedores.
- Indicadores de contratación: tipología, importes, etc
- Inventario de bienes inmuebles y muebles: bienes patrimoniales, vehículos, número de líneas móviles corporativas, etc
- Información relativa a viajes, dietas y gastos derivados por parte de los órganos de gobierno unipersonales.
- Porcentaje de financiación de la respectiva Comunidad Autónoma
- Datos económicos de las entidades participadas (fundaciones, etc.)
- Coste de las campañas de publicidad y de promoción institucional y relaciones públicas
- Gastos globales abonados en concepto de gratificaciones extraordinarias y de indemnizaciones por razón del servicio
- Patrocinio y mecenazgo
- Importe comprometido en los convenios suscritos
- Gastos de atención protocolaria
- Coste de coches oficiales y de catering de reuniones
- Importe que la Universidad invierte anualmente en el desarrollo de políticas de igualdad de género y visibilidad del colectivo LGTBIQ
- Gasto económico desglosado que supone cada uno de los procesos electorales celebrados en un curso académico por la Universidad
- Gastos de celebración de cursos de verano.
- Financiación aportada por la Comunidad Autónoma y por organismos nacionales e internacionales
- Gastos de consumo energético
- Número de encomiendas de gestión, importes y entidades con la condición de medio propio en la Universidad
- Subvenciones recibidas por la Universidad (importes y entidad concedente)

¹⁶ Véase asimismo la [nota a pie 1](#) de la presente guía.

6.2. GASTOS

- *Acceso a los pagos realizados a empresas, en un determinado periodo, con los datos de la empresa, importe y fecha, y a las facturas correspondientes a contratos menores de un centro académico*

Cuando se trate de una persona jurídica se facilitará la información al no resultar de aplicación la normativa en materia de protección de datos personales.

Si se trata de una persona física en el ejercicio de su actividad comercial se realizará el juicio de ponderación previsto en el art. 15.3 de la LTAIBG. Con carácter general, prevalecerá el interés público en la divulgación, teniendo en cuenta que se trata del escrutinio del buen uso de los fondos públicos¹⁷, dejando a salvo aquellos supuestos que por las circunstancias específicas se aprecie que debe prevalecer el derecho de protección de datos del empresario. En cualquier caso, atendiendo al principio de minimización, parece razonable ocultar el dato del domicilio de la empresa de la persona física, ya que en empresas familiares podría coincidir con su domicilio particular, sin que este dato aporte nada para el fin de transparencia pretendido.

- *Acceso por parte de un miembro de un órgano de gobierno a datos personales en materia económica y contable relativa a un Centro (dietas devengadas, etc.)*

Si se trata de datos que afectan a los órganos de gobierno unipersonales, se recomienda que se haga pública la información en cuestión, teniendo en cuenta el interés general en el escrutinio de los fondos por quienes ocupan puestos de relevancia en la gestión universitaria.

Para el resto de supuestos, la comunicación de datos al solicitante se ha de limitar a la finalidad que la justifique; es decir, en la medida en que los datos de carácter personal facilitados sean necesarios, adecuados y pertinentes para el ejercicio de las funciones que le corresponden como miembro del respectivo órgano de gobierno, siempre que no haya circunstancia alguna que pueda interferir en la esfera íntima del titular de los datos.

6.3. CONTRATOS

- *Acceso a datos de los pliegos, licitación, adjudicación y contratos sujetos a la Ley de Contratos del Sector Público*

Se concede en virtud de la correspondiente ley de transparencia (publicidad activa) y Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (art. 63). Se puede consultar en el perfil del contratante.

- *Acceso a datos de las primas pagadas a las entidades aseguradoras, mutuas de accidentes, etc., en un determinado periodo de tiempo*

Al tratarse de personas jurídicas se facilitará la información al no resultar de aplicación la normativa en materia de protección de datos personales.

- *Publicación de datos en el perfil del contratante*

En la publicación de la información relativa a los procedimientos de contratación pública como consecuencia del cumplimiento de las obligaciones de transparencia establecidas en la Ley 9/2017, la APD-Cat afirma que la difusión de datos personales identificativos debería abarcar sólo el nombre y apellidos

¹⁷ El CTBG estima el acceso a la copia de un contrato menor, argumentando que versa su objeto sobre "actos de gestión administrativa con repercusión económica o presupuestaria" en materia contractual de publicación obligatoria (RT 0386/2018).

de los licitadores y adjudicatarios, así como el nombre, apellidos y cargo del trabajador público que interviene por razón del cargo o funciones, al ser esta la información mínima necesaria para lograr la finalidad pretendida -artículo 5.1.c) RGPD- ([dictamen CNS 1/2019](#)).



Buena práctica: difundir la información sobre los procedimientos de contratación administrativa a través de los correspondientes perfiles del contratante solo con los nombres y apellidos de los adjudicatarios, licitadores, etc., sin firma y sin ningún otro dato personal adicional.

6.4. ACCESO A DATOS RETRIBUTIVOS

Los datos correspondientes al sueldo, el complemento de destino y el complemento específico se incluyen cada año en la Ley de Presupuestos Generales del Estado y correspondientes leyes autonómicas. Por ello, tratándose de información pública y no asociada a un empleado público concreto, no hay ninguna limitación para que las solicitudes de acceso que se refieran a los mismos sean concedidas. Además, sin perjuicio de lo que establezca la legislación autonómica de transparencia que sea de aplicación en cada caso, el art. 8.1.f) LTAIBG establece que *“Las retribuciones percibidas anualmente por los altos cargos y máximos responsables de las entidades incluidas en el ámbito de la aplicación de este título. Igualmente, se harán públicas las indemnizaciones percibidas, en su caso, con ocasión del abandono del cargo”*.

En lo que respecta al acceso a la restante información de naturaleza retributiva, hay que estar, como manifiestan la CTBG y la AEPD ([dictamen conjunto de 23 de marzo de 2015](#)), a lo siguiente:

- a. Si la información sobre las retribuciones asignadas a un determinado puesto de trabajo contiene categorías especiales de datos (art. 9.1 RGPD), solo podría facilitarse el acceso en los términos establecidos en el apartado 1 del artículo 15 de la LTAIBG.
- b. En la información referente a los puestos de trabajo de mayor nivel de responsabilidad (incluidos personal eventual y personal de libre designación en orden decreciente en función de su nivel de responsabilidad) y mayor autonomía en la toma de decisiones o a aquellos cuya provisión se realice con un cierto grado de discrecionalidad o se justifique en la existencia de una especial relación de confianza prevalecerá, como regla general, el interés público sobre la protección de datos y la intimidad.

En cualquier caso, la información deberá referirse a las retribuciones íntegras anuales, sin excluir las deducciones que fueran aplicables ni desglosar los distintos conceptos retributivos (ya que pueden incidir en la intimidad de la persona), salvo que así se solicitase expresamente, en cuyo caso, debería analizarse la situación del empleado público en cada caso concreto.

En su [dictamen conjunto de 24 de junio de 2015](#), la CTBG y la AEPD matizan al respecto que no se facilitará la información *“cuando el acceso afecte a uno o varios empleados o funcionarios públicos que se encuentren en una situación de protección especial –p. ej. la de víctima de violencia de género o la de sujeto a una amenaza terrorista-, que pueda resultar agravada por la divulgación de la información relativa al puesto de trabajo que ocupan”*.

- c. En cuanto a los puestos de menor nivel de responsabilidad y autonomía o a los puestos cuya provisión se verifica por procedimientos reglados o no implican una relación de especial confianza, prevalecerá, también con carácter general, el respeto a la protección de datos y a la intimidad. Por todas, [resolución 28/2018](#) del Consejo de Transparencia de Aragón (en adelante, CTA).

7. CONVENIOS

7.1. ACCESO AL CONTENIDO

Se recomienda que su publicación se haga en la intranet (con acceso limitado a los miembros de la comunidad universitaria) omitiendo aquellos datos personales acordes con el principio de minimización (DNI de los firmantes, rúbrica, etc.), al no ser necesarios para alcanzar la finalidad pretendida. En este sentido, la AEPD sostiene que *“teniendo en cuenta los requisitos exigidos por su artículo 8.1 b) [LTAIBG], cabe concluir que éste último precepto no otorga cobertura a la inclusión en el documento escaneado de los convenios o encomiendas de gestión de la firma manuscrita de los intervinientes”* (informe 0502/2014).

El Consejo de Transparencia y Protección de Datos de Andalucía (en adelante, CTPDA) entiende que procede el acceso a la copia de un convenio, salvo que haya algún límite que lo impida, sin que sea suficiente indicar el enlace donde consta la relación de convenios suscritos en virtud de la obligación de publicidad activa (R 77/2018).

No se facilitará el acceso cuando concurren circunstancias excepcionales que hagan necesario preservar la confidencialidad de la información que contenga.

Si la publicación se hace en abierto se han de observar las prevenciones indicadas anteriormente.

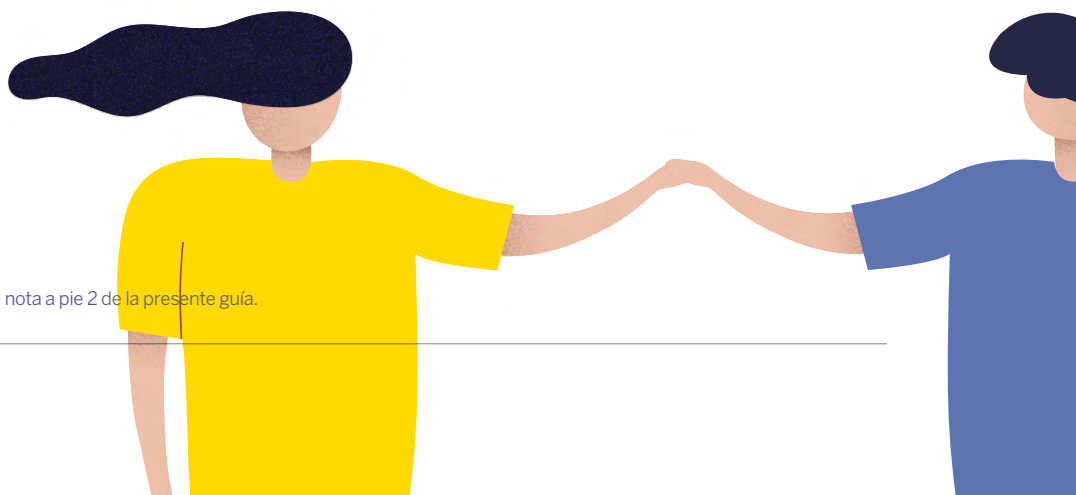


Buena práctica: en cualquier caso, salvo que se opongan circunstancias excepcionales singularizadas, si se desea consultar el documento en su integridad puede indicarse un aviso en la página web de la Unidad donde puede realizarse la consulta.

7.2. ACCESO A DATOS AGREGADOS RELATIVOS A CONVENIOS

Sin perjuicio de la obligación de transparencia contenida en la LTAIBG y, en su caso, en las leyes autonómicas de transparencia, puede facilitarse a quien lo solicite toda información disociada o anonimizada (aquella que no guarde relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo), como por ejemplo el número de alumnos que se han acogido a los convenios de prácticas curriculares y extracurriculares entre la Universidad y empresas, promedio de duración de estas y salarios medios abonados¹⁸.

¹⁸ Véase asimismo la nota a pie 2 de la presente guía.



8. PROCESOS ELECTORALES

8.1. PUBLICACIÓN DE CENSOS. ASPECTOS GENERALES

Se recomienda que su publicación se haga en la intranet, pudiendo cada elector consultar solo los electores pertenecientes a su respectivo sector o, en su caso, circunscripción, salvo que el propio régimen electoral de la Universidad prevea estatutaria o reglamentariamente la publicación conteniendo todos los electores de cada sector o, en su caso, circunscripción. Si además está establecido que se haga en tabloneros de anuncios físicos, se debe actuar de la siguiente forma:

- a. Preservar la documentación a través de tabloneros cerrados con llave y, si no es posible, se monitorizará la información personal publicada evitando que la documentación pueda ser retirada por personas no autorizadas.
- b. Evitar su ubicación en zonas de acceso a los centros o en lugares de paso.
- c. Proceder a su inmediata retirada en el momento en el que se hayan cumplido los plazos de reclamaciones.

Sea cual sea el modo de publicación, habrá que atenerse a lo previsto en la disposición adicional séptima de la LOPDGDD, tal y como se indica en la [Orientación para la aplicación provisional de la Disposición Adicional Séptima de la LO 3/2018](#), aprobada por la AEPD.



Buena práctica: en caso de publicarse en soporte físico y siempre que no se pueda garantizar el cierre con llave o la monitorización, se aconseja estudiar, si la norma interna de cada Universidad no lo impide, la sustitución del tablón por su consulta controlada en la propia Secretaría o Conserjería de cada Centro.

8.2. PUBLICACIÓN DE MIEMBROS DE LAS MESAS ELECTORALES

Se reproduce lo indicado en el subepígrafe anterior.

8.3. COMUNICACIÓN DE DATOS CENSALES A LAS CANDIDATURAS

Cuando resulte de aplicación de forma supletoria el art. 41.5 de la LOREG, la base jurídica de la comunicación será el interés público –art. 6.1.e) RGPD.

Como señala la AEPD, “*siempre que el acceso a los datos se produzca exclusivamente durante la campaña electoral y los datos sean únicamente utilizados a los fines previstos en la propia legislación electoral sería posible el tratamiento de los datos, sin que cupiera, en principio, que el interesado manifestase su negativa al tratamiento, procediéndose en todo caso a la cancelación de los datos al término de la campaña*” (informe 0244/2014).

Sin embargo, excepcionalmente y por razones debidamente justificadas, podrá excluirse a las personas que pudieran ser objeto de amenazas o coacciones que pongan en peligro su vida, su integridad física o su libertad, de las copias del censo electoral (art. 41.6 LOREG).

La AEPD estima que “*Fuera de estos casos, en que además el ejercicio se prevé como anterior a la cesión y no ejercido ante la candidatura, el régimen actualmente vigente no permite invocar el citado derecho de oposición a la recepción de publicidad electoral*” (informe 0244/2014).

8.4. PUBLICACIÓN DEL CENSO DE LAS ELECCIONES SINDICALES DE PERSONAL FUNCIONARIO

Señala la APDCat que conforme a la normativa de aplicación “es legítimo que el órgano competente recoja los datos personales consistentes en el nombre y dos apellidos, el DNI (o NIF), la fecha de nacimiento y la antigüedad de los trabajadores de una unidad electoral para la celebración de las elecciones a los órganos de representación de los trabajadores en las Administraciones públicas.

Sin embargo, desde el punto de vista de la normativa sobre protección de datos, se considera que la publicación de los datos consistentes en el DNI (o NIF), la fecha de nacimiento y la antigüedad de estos trabajadores en el tablón de anuncios de la unidad electoral correspondiente puede vulnerar el derecho a la protección de datos personales de los electores, ya que estos datos no son necesarios para el cumplimiento de la finalidad primera de la publicación de las listas de electores, que no es otra que saber si un funcionario se considera o no elector” (dictamen CNS 18/2008).

Por lo expuesto, no parece que se ajuste al principio de minimización la publicación del nombre y apellidos acompañado del DNI, fecha de nacimiento y antigüedad en soporte físico, teniendo en cuenta que los tabloneros de anuncios pueden ser consultados por cualquier ciudadano que transite por el lugar de exposición, y que esos datos no determinan la condición de elector o elegible. En cualquier caso, de publicarse el DNI o documento identificativo equivalente (p.e. en casos de coincidencia de nombre y apellidos), habría que atenerse a lo previsto en la Disposición Adicional Séptima de la LOPDGDD, tal y como se indica en la [Orientación para la aplicación provisional de la Disposición Adicional Séptima de la LO 3/2018](#), aprobada por la AEPD.



Buena práctica: atender a las recomendaciones indicadas en el [subepígrafe 8.1](#).

8.5. PUBLICACIÓN DEL CENSO DE LAS ELECCIONES SINDICALES DE PERSONAL LABORAL

A diferencia del supuesto anterior, los datos de edad y antigüedad en la empresa sí determinan la condición de elector y elegible, por lo que sería de aplicación el mismo razonamiento indicado anteriormente pero con la salvedad de la publicación, junto al nombre y apellidos, de la edad y antigüedad en la empresa.



Buena práctica: atender a las recomendaciones indicadas en el [subepígrafe 8.1](#).

8.6. ACCESO A LAS COPIAS DE LAS ACTAS DE LAS MESAS EN LAS ELECCIONES A ÓRGANOS COLEGIADOS

Como recuerda el CTBG, prevalece el escrutinio y transparencia en la acción de los responsables públicos (RT/0272/2018), por lo que procedería estimar el acceso siempre que se atienda al principio de minimización (p.e. no resulta necesario para atender al principio de transparencia en la actuación administrativa la firma de los que las suscriben).



Buena práctica: ofrecer la información solo con nombre y apellidos de los firmantes.

9. PRIVACIDAD Y DERECHO DE DEFENSA

9.1. DATOS AGREGADOS¹⁹

Puede facilitarse a quien lo solicite toda información disociada o anonimizada (aquella que no guarde relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo), como, por ejemplo:

- Número de recursos administrativos, contenciosos-administrativos y demandas laborales interpuestos en un periodo de tiempo determinado, desglosados por colectivo
- Número de resoluciones administrativas y judiciales firmes estimatorios en todo o en parte en un periodo de tiempo, desglosados por colectivo
- Costas judiciales en los diferentes procesos judiciales en un periodo de tiempo determinado
- Número de expedientes de responsabilidad patrimonial que han concluido con resolución estimatoria, así como cantidades concedidas, en un periodo de tiempo determinado
- Tipología de causas de apertura de expedientes de responsabilidad patrimonial en un periodo de tiempo determinado



¹⁹ Véase asimismo el segundo párrafo del subepígrafe 1.2 de la presente guía.

9.2. NOTIFICACIÓN DE RESOLUCIONES A TERCEROS AFECTADOS

Cuando se notifique la interposición de un recurso administrativo a personas que pudieran ver afectados sus derechos e intereses por la citada impugnación, se debe de ocultar todos los hechos y datos que no resulten relevantes para la tutela en cuestión (p.e. datos de domicilio familiar, teléfono personal, nombre y apellidos y demás datos personales de terceros que no interfieran ni directamente ni indirectamente en la tutela de sus derechos).

9.3. PUBLICACIÓN DE RESOLUCIONES JUDICIALES

En cuanto a las resoluciones judiciales, como recuerda la AEPD *“las sentencias no son públicas en cuanto no se prevé la publicidad de las mismas, solo son accesibles a las partes interesadas, y su publicación oficial por el Consejo General del Poder Judicial se hace en internet anonimizando los datos de carácter personal o cualquier dato que pueda hacer identificable a la persona”* (resolución PS/0058/2017). En análogo sentido se pronuncia la autoridad de control en su [resolución AP/0002/2017](#).

La AEPD subraya que *“[...] la colisión entre la publicidad de las sentencias y el derecho a la intimidad de las personas ya ha sido, por otra parte, analizado por el Consejo General del Poder Judicial, disponiendo en el Acuerdo de 18/06/1997, por el que se modifica el Reglamento número 5/1995, de 7/06, regulador de los aspectos accesorios de las actuaciones judiciales, como apartado 3 del nuevo artículo 5 bis del Reglamento, que ‘En el tratamiento y difusión de las resoluciones judiciales se procurará la supresión de los datos de identificación para asegurar en todo momento la protección del honor e intimidad personal y familiar’[sin perjuicio de haber sido objeto de estudio por parte de la jurisprudencia]”*(resolución AP-00064/2007).

Por ello, en aquellos casos en que se deban hacer públicas resoluciones judiciales en abierto en la página web de la universidad, siempre que no se cuente con el consentimiento expreso de la persona o personas afectadas, será necesaria la realización de un proceso de disociación que impida que la persona sea identificada o identificable. En este sentido, como advierte la AVPD no puede darse una solución unívoca, pues habrá ocasiones en las que *“será suficiente con la supresión del nombre y los apellidos, pero en otras, puede resultar necesario suprimir aquellas informaciones que, sin ser de por sí identificativas, permitan al lector de la sentencia identificar a las partes, a alguna de ellas o a personas intervinientes en el proceso, bien por la localización geográfica citada, por las descripciones contenidas en el relato de hechos, o por las circunstancias concurrentes en el caso [...]”* (dictamen CN 16-007).



Buena práctica: que solo se divulgue un anuncio de publicación de la correspondiente resolución sin asociarla con datos personales, informando que la consulta del texto completo podrá ser realizada contactando con el Servicio o Unidad competente de cada Universidad. Esta misma práctica es aconsejable cuando se publique en el Tablón Edictal Único del BOE el anuncio al que se refiere el primer párrafo del art. 44 LPACAP.

Buena práctica: si solo afecta a derechos e intereses de miembros de la comunidad universitaria, es aconsejable que su acceso sea restringido (intranet) al concreto colectivo que pueda verse afectado, ocultando aquellos datos personales, hechos y circunstancias que no sean adecuados y pertinentes en el caso concreto para la tutela de sus derechos e intereses.

9.4. PRÁCTICA DE LAS NOTIFICACIONES EN PAPEL

En cuanto a la práctica de las notificaciones en papel, mientras estas subsistan, se recomienda que se evite cualquier indicación en los sobres o en las hojas de acuse de la que se infiera, directa o indirectamente, una situación personal o familiar. Por ejemplo, no es aconsejable indicar en parte visible términos que pueden afectar a la intimidad como “embargo, multa, etc.”. Mismo modo de proceder se ha de adoptar en las notificaciones en el tablón edictal único del BOE, procurando no incluir información que, sin ser imprescindible para el fin perseguido con la notificación, pueda afectar a la intimidad personal o familiar del interesado.

9.5. CONSULTA Y COPIA DE EXPEDIENTES DE PROCEDIMIENTOS SELECTIVOS

- *Acceso por quien tiene la condición de interesado en el procedimiento*

De conformidad con lo previsto en el artículo 53.1.a) LPACAP, si se es persona interesada se tiene derecho a acceder y a obtener copia de los documentos contenidos en los citados procedimientos. En este sentido, el CTA entiende que “[...] no es exigible el consentimiento de aquellas personas que participen en un procedimiento de concurrencia competitiva, ni para el tratamiento de las calificaciones obtenidas en dicho procedimiento, ni para la entrega de copia de sus exámenes aprobados, y ello como garantía y exigencia de los demás participantes para asegurar la limpieza e imparcialidad del procedimiento en el que concurren [...]”, por lo que tratándose de un procedimiento de concurrencia competitiva “un opositor tiene derecho a obtener copia del examen de otro opositor participante en el mismo proceso selectivo, tratándose de un examen aprobado” (R 7/2019; R 23/2017)²⁰. En términos análogos, el CTBG estima que se facilite la puntuación en cada uno de los méritos aportados por los candidatos presentados al premio nacional de fin de carrera de una titulación en la que el solicitante es persona interesada (R 097/2019).

Cabe realizar la puntualización de que la doctrina del CTBG considera que no resulta correcta la inadmisión de una solicitud de acceso a la información pública en base a lo dispuesto en la disposición adicional primera, apartado 1 LTAIBG, por quien es interesado en un procedimiento que está en vía de recurso pero que ha finalizado con la correspondiente resolución definitiva de adjudicación de plazas²¹, por lo que procede que se le facilite “la información relevante del proceso selectivo que le permita comprobar la imparcialidad del procedimiento en el que concurren, incluidos los datos de carácter personal de terceros también participantes en el mismo proceso selectivo con los que la solicitante compite por las mismas plazas” (R 119/2019).

En cuanto al acceso a criterios cualitativos establecidos por las comisiones de selección, constando en el expediente la documentación relativa al estudio, debate y aprobación de las preguntas aportadas por los miembros del tribunal en cada uno de los ejercicios, así como los criterios cualitativos que fueron establecidos o seguidos para valorar el acierto o desacierto de los candidatos en cada uno de los ejercicios deberían ser facilitados al solicitante, atendiendo al principio de transparencia en el desarrollo del proceso.

Si no existen actas o documentos con la información que se solicita, no puede accederse a su contenido, al no constituir información pública en poder de la Administración, conforme a lo dispuesto en los artículos 12 y 13 LTAIBG, como pone de manifiesto el CTBG (R/0381/2016).

²⁰ En sentido similar se pronuncia el Consejo de Transparencia de Navarra (en adelante, CTN) (Acuerdo AR/15/2018).

²¹ Por todas, R/206/2019; R/0159/2016. La GAIP, en su resolución 17/2015, también aboga por esta interpretación de lo que se entiende por procedimiento finalizado. Asimismo, en su dictamen 7/2016, el citado órgano ofrece un criterio interpretativo sobre la condición de interesado en un procedimiento, a los efectos de establecimiento del procedimiento a seguir en las peticiones de acceso a información pública.

Dicho todo lo anterior, también hay que tener en cuenta que se trate de ejercitar el derecho previsto en el art. 53.1.a) LPACAP o el derecho de acceso a la información pública, ambos tienen que compatibilizarse con la legislación en materia de protección de datos (RGPD y LOPDGDD).

En concreto, de acuerdo con lo previsto en el artículo 5.1.c) del citado RGPD los datos que sean objeto de tratamiento han de ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados “principio de minimización de datos”. Por todo ello, no sería conforme con el citado principio relativo al tratamiento de datos personales una revelación indiscriminada de datos personales de otros participantes, ya que han de circunscribirse a aquellos que sean necesarios para el ejercicio del derecho de defensa de la persona interesada en vía administrativa o judicial por afectar a su esfera jurídica (por todas, resolución de la GAIP 17/2015).

A título de ejemplo, señala el CTA que “[...] no puede apreciarse interés público en la divulgación de los datos identificativos y notas de aquellos candidatos que no han aprobado en un proceso selectivo, puesto que no proporcionan elemento comparativo alguno, ya que no se encuentran en una situación de ventaja –aprobado– en el proceso selectivo respecto a quien solicita la información” (R 35/2018).

En esta línea, recuerda la APDCat, que se ha de excluir la documentación que contenga datos personales especialmente protegidos, así como aquellos datos que resulten innecesarios para alcanzar la finalidad perseguida (IAI 49/2018; IAI 51/2017). Al respecto, la AEPD sostiene que en un procedimiento selectivo (como lo es la admisión de estudiantes de nuevo ingreso en una determinada titulación), de acuerdo con el principio de transparencia, resultaría justificado el acceso únicamente por parte de los interesados a datos sensibles como las personas que han participado por el turno de discapacitados (datos de salud de los afectados), y siempre limitándolo a los datos personales mínimos imprescindibles (resolución E/05037/2014).

A mayor abundamiento, la aplicación del principio de minimización debe llevar a concluir que, siempre que el examen directo -sin tener que hacer copia de la documentación del resto de aspirantes- permita alcanzar la finalidad perseguida con el acceso por el interesado, habría que decantarse por esta opción (dictamen CNS 68/2015).



Buena práctica: exigir la firma de un compromiso de confidencialidad del uso de los datos personales comunicados para el fin exclusivo del ejercicio del derecho de defensa, si bien su no firma no exime al destinatario de la información de estar sujeto a la normativa en materia de protección de datos en el tratamiento posterior que haga de los datos personales.

- *Acceso por quien no tiene la condición de interesado en el procedimiento*

Si se pretende el acceso a datos personales, sería necesario realizar la ponderación entre el interés del solicitante y el derecho a la protección de datos personales de los participantes en el concreto proceso selectivo, y en función de este ejercicio ponderativo se determinará -atendiendo a las circunstancias específicas de cada caso- cuál de ambos debe prevalecer.

La doctrina más reciente aboga, como regla general, por la limitación del citado acceso a la información pública, cuando se trate de datos personales de los participantes en el procedimiento. Por ejemplo, el CTN afirma que “La revelación a terceros no aspirantes de los exámenes en una oposición, de las programaciones didácticas elaboradas y de los guiones utilizados, así como de otros documentos que contengan evaluaciones de ejercicios realizados, puede afectar al derecho a la intimidad de las personas aspirantes y a su derecho al honor” (Acuerdo AR 10/2019). Por su parte, el CTBG -en un caso relativo al acceso a las puntuaciones de los candidatos con el fin de confirmar que las distintas comisiones evaluadoras para la concesión de premios nacionales de fin de carrera han valorado de la misma forma méritos análogos- determina que al no existir concurrencia entre el solicitante y los afectados por la

solicitud debido a que la convocatoria establece compartimentos estancos en las distintas ramas de conocimiento para la adjudicación de los premios, prevalece el derecho a la protección de datos de los afectados (R 038/2019).

- *Acceso a cuadernos de exámenes de pruebas selectivas y plantillas u hojas de respuesta*

El CTBG se ha pronunciado en diversas resoluciones sobre el asunto siendo favorable a la estimación, con carácter general, del acceso a esta información, salvo que a la vista del caso concreto se acredite algún límite para el acceso o exista causa de inadmisión²².

Si se solicita además el acceso a los casos prácticos, o preguntas de desarrollo, y si existe la solución correcta de los casos prácticos o de las citadas preguntas, como advierte el CTBG, se debe proporcionar al reclamante la identificación de los elementos mínimos que debe contener la respuesta al caso práctico planteado o las posibles soluciones que haya realizado previamente el Tribunal al objeto de calificar los casos prácticos realizados o, por el contrario, confirmar que se carece de dicha identificación previa y, por lo tanto, que no existen criterios en los que se haya basado el Tribunal para adoptar su decisión (R/00016/2019; R/0063/2018; R/0004/2007; R/0042/2017)²³.

Cuestión distinta es la pretensión de acceso a las plantillas concretas individualizadas de cada ejercicio y aspirante por parte de quien no es parte interesada, que debe ser desestimada, ya que solo a los participantes le corresponde comprobar la imparcialidad del procedimiento en que concurre, incluidos los datos de terceros participantes en el mismo proceso selectivo con los que compite por las mismas plazas, siempre que éstos hayan resultado aprobados y ello afecte a la necesaria concurrencia competitiva, como señala la Comisión Vasca de acceso a la información pública (R/033/2018).

- *Acceso a copias de actas y otra documentación correspondiente a procesos selectivos*

El principio de transparencia debe ser interpretado de forma conjunta con la legislación en materia de protección de datos personales. Por ello, con carácter general, el acceso a la información pública de personas no interesadas en el procedimiento se realizará previa disociación de los datos personales.

La GAIP puntualiza que “[...] el hecho de conocer las actas cuando ya ha tenido lugar la reunión que el acta refleja y el tribunal ya ha llevado a cabo las deliberaciones y ha adoptado los acuerdos de que dan constancia no afecta al proceso de toma de decisión de estos; [...] sin que pueda servir “para revelar anticipadamente el contenido de las pruebas que se deben realizar en una fase posterior del proceso selectivo, ya que ello desnaturalizaría el sentido y la finalidad selectiva de la prueba [...]” (R 162/2017).

Sin embargo, si se trata de acceder, por ejemplo, a los criterios específicos del baremo de una plaza de profesorado o a cualquier otra documentación contenida en el expediente en la que no existan datos personales debe prevalecer el interés público en escrutar la transparencia del proceso, ya que como recuerda el CTPDA “en lo que se refiere a la gestión de recursos humanos de los empleados sujetos al sector público las exigencias de transparencia de la información deben ser escrupulosamente atendidas, pues, además de suponer un evidente gasto de fondos públicos, los procesos selectivos correspondientes han de estar basados en los principios de igualdad, mérito y capacidad” (R 122/2016).

²² Por todas, RT 0001/2019; R/00016/2019; R/0145/2019; RT 0155/2019; RT 0417/2018; RT 0472/2018; RT 0473/2018; RT 0476/2018; R/0530/2018; R/0004/2007; R/0061/2016. En idéntico sentido estimatorio abogan la mayoría de organismos autonómicos de transparencia, como el CTPDA (R 113/2017), el CTA (R 13/2019), la GAIP (R 174/2018) y el CTN (Acuerdo AR/17/2018).

²³ De forma complementaria, el CTBG afirma que, estando documentados los criterios utilizados por un tribunal para la evaluación de un ejercicio ya concluido correspondiente a pruebas selectivas de acceso, la solicitud de acceso ha de ser estimada al haber servido esa información documentada para la calificación de un ejercicio que ya ha concluido, y a que el acceso a la misma facilita el conocimiento de la decisión pública adoptada (R/0341/2017). En términos análogos también se pronuncia el CTN, al referirse a las anotaciones o notas auxiliares de los miembros del Tribunal calificador, si están incorporadas al expediente, pues en ese caso habrán adquirido relevancia pública e interés público (Acuerdo AR/15/2018).



En lo que respecta al acceso por parte de quienes ostentan la condición de interesados puede consultarse lo indicado en el siguiente [enlace](#).

- *Acceso a los criterios técnicos utilizados para otorgar puestos de libre designación y al currículum de los candidatos*

De acuerdo con el principio de transparencia procede el acceso a los criterios utilizados para la provisión de este tipo de puestos. Así lo señala el CTBG en su resolución [R/0498/2018](#).

Respecto al acceso a los currículos de los diversos aspirantes, prevalecería el derecho a la protección de datos de aquellos que no han conseguido la adjudicación. Apunta al respecto el CTPDA que *“el acceso a los currículos de los aspirantes que no han obtenido el puesto conlleva un sacrificio de su privacidad que resulta excesivo para la satisfacción del interés público inherente a la divulgación de la información solicitada. Asimismo, la revelación de los currículos de la totalidad de los aspirantes, como apunta el órgano reclamado, podría tener efectos disuasorios en futuras convocatorias, afectándose así potencialmente a la concurrencia -sin duda conveniente- en estos procedimientos y, con ella, el interés público de la propia Administración”*.

Por el contrario, el citado Consejo estima que el interés público en la divulgación de información relativa a una persona nombrada para un puesto no directivo de libre designación de nivel 30, 29 o 28, o equivalentes, debe prevalecer, con carácter general, sobre su interés individual en la preservación de la intimidad y los datos de carácter personal. Por ello, procedería el acceso al currículum para que pueda ser conocido el perfil profesional, académico, formativo y similares de la persona adjudicataria del puesto, pero no otros datos meramente personales tales como el documento nacional de identidad, fecha de nacimiento, el domicilio, la dirección, el número de teléfono, correo electrónico, estado civil, número de hijos, fotografía, etc., y, por supuesto, cualquier otro dato que esté especialmente protegido ([R 66/2016](#)).

- *Acceso por los representantes de los trabajadores*

Los representantes de los trabajadores ejercen un control del cumplimiento de la normativa en ámbito laboral, que incluiría la posibilidad de poder contrastar y corroborar el uso adecuado del amplio margen de discrecionalidad que conllevan los procedimientos de provisión. La APDCat indica que *“[...] conocer la puntuación que ha obtenido una persona candidata en relación con la experiencia profesional, la formación académica o en relación a la entrevista realizada, en caso de haberse realizado, daría suficiente información si lo que se pretende es detectar posibles actuaciones arbitrarias por parte del órgano encargado de hacer la selección, el cual debe actuar dentro los parámetros de imparcialidad y de discrecionalidad técnica que se le atribuyen (art. 55.2, apartados c) y d) TRLEBEP), sin que la normativa de protección de datos personales impida dar acceso al representante de los trabajadores a la información referida a la valoración del tribunal en relación con los candidatos que han sido escogidas para formar parte de la bolsa de trabajo, y en la puntuación otorgada a los candidatos seleccionados.*

Esto, sin perjuicio de que si las actas del tribunal calificador incorporan datos de salud u otros que puedan revelar cualesquiera otros datos de categorías especiales de datos, para el acceso a estos deberá disponerse del consentimiento de las personas afectadas” (informe IAI 11/2017).

Asimismo, como advierte la GAIP, *“[...] considerando las consecuencias negativas que una filtración podría tener para el fin último del propio proceso selectivo, y teniendo en cuenta que los representantes de los trabajadores podrán acceder plenamente a la misma [contenido de la entrevista] una vez terminen las entrevistas, se les debe denegar temporalmente el acceso a esta parte del acta” (R 162/2017).*

10. RÉGIMEN DISCIPLINARIO

10.1. DATOS AGREGADOS ²⁴

Puede facilitarse a quien lo solicite toda información disociada o anonimizada (aquella que no guarde relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo), como por ejemplo:

- Número de expedientes disciplinarios, desagregados por colectivos, en un periodo determinado, diferenciado los resueltos estimatoria y desestimatoriamente, y en su caso cuántos han sido objeto de impugnación en vía judicial
- Número de informaciones reservadas abiertas y porcentaje de las que no dan lugar a la incoación de expediente disciplinario, en un periodo de tiempo determinado
- Número de denuncias presentadas en un periodo determinado, desglosando cuántas han sido archivadas o han dado lugar a la incoación de expediente disciplinario
- Tipología de infracciones investigadas y sanciones firmes en un periodo de tiempo determinado
- Número de denuncias presentadas por acoso de índole sexual y/o laboral, en un periodo de tiempo determinado, diferenciado el tipo de acoso y el colectivo
- Número de veces que se ha activado el protocolo de actuación contra el acoso y el resultado final (archivo, traslado a la Inspección de Servicios)



²⁴ Véase asimismo el segundo párrafo del subepígrafe 1.2 de la presente guía.

10.2. ACCESO A DATOS DE DENUNCIA E IDENTIDAD DEL DENUNCIANTE

Por lo que respecta a los datos del denunciante, cuando se haya iniciado un procedimiento disciplinario, el denunciado en su condición de interesado en el mismo tendrá, con carácter general, derecho a conocer el estado de la tramitación del expediente y a obtener copia de los documentos que contenga, incluida la identidad de la persona denunciante-art. 6.1.f) RGPD-, sin que sea acorde la comunicación de datos personales que obren en el expediente cuyo conocimiento no sea relevante para el ejercicio de los derechos del interesado. Por ello, como advierte la AEPD, *“si resultara evidente la necesidad de que el imputado conociera la identidad de los denunciantes para el ejercicio del derecho de defensa, habrían de incluirse tales datos identificativos”*. No obstante, la autoridad de control puntualiza que *“si la denuncia no formara parte del expediente administrativo no existirá obligación por parte de la consultante de poner en conocimiento del denunciado ni la existencia de una denuncia previa ni la identidad del denunciante”* (informe 0342/2012).

10.3. ACCESO A INFORMACIÓN RESERVADA

La información reservada es un procedimiento destinado a la averiguación y esclarecimiento de hechos que pudieran alcanzar, en su caso, relevancia disciplinaria y la determinación, en su caso, de los posibles responsables, sin que revista por sí misma naturaleza de procedimiento sancionador o disciplinario contra persona alguna. De acuerdo con ello, si no se incoa expediente disciplinario como consecuencia de dicha información reservada no existirán personas interesadas en el mismo, por lo que no procedería el acceso a dicha información²⁵. Si, por el contrario, se incoara expediente disciplinario como consecuencia de la información reservada y ésta no se hubiese incorporado al expediente, habrá derecho de acceso a la misma en la medida en que pudiese afectar al derecho a la defensa (STS núm. 2838/1998, de 5 de mayo) (R 1998\4624), salvo en los casos en que las circunstancias alegadas por los afectados en el trámite de audiencia hagan aconsejable preservar su privacidad (informe IAI 22/2018).

Tampoco se tiene la condición de persona interesada en los términos previstos en la normativa de procedimiento administrativo -art. 4 y art. 53.1.a) LPACAP- si el expediente de información previa ha concluido con el archivo de las actuaciones. Como afirma la APDCat, *“[...] se podría informar a la persona denunciante sobre el hecho de que se ha producido el archivo del expediente. Más allá de esto, habría que denegar el acceso al expediente de información reservada, salvo si las personas afectadas dan su consentimiento”* (dictamen CNS 42/2018).

10.4. ACCESO A DATOS PERSONALES EN CASO DE ACTIVACIÓN DEL PROTOCOLO PARA LA PREVENCIÓN, DETECCIÓN, Y ACTUACIÓN EN RELACIÓN CON LOS CASOS QUE AFECTAN A LA DIGNIDAD Y LA DISCRIMINACIÓN EN EL TRABAJO

Si lo que se pretende es la consulta o la obtención de copia de los documentos que integran el expediente administrativo, y que pudieran afectar a los derechos e intereses de quien los solicita, debería de aplicarse en el tratamiento de la información las mismas reglas que se aplican a la información reservada, por la propia naturaleza de estas actuaciones. Por ello, como sostiene la APDCat, el derecho de acceso podría verse limitado mientras duren las actuaciones de investigación y siempre que se considere que puede suponer un perjuicio para la investigación de conductas que podrían ser sancionadas en vía administrativa o incluso en vía penal -limitación prevista en el artículo 23.1 d) del RGPD y art. 14.1.e) de la

²⁵ Además, tratándose aún de un expediente que no está terminado, el acceso podría perjudicar las facultades de investigación, inspección, vigilancia y control, un perjuicio previsible, y no meramente hipotético, por lo que concurriría la causa de inadmisión prevista en el art. 14.1 g) de la LTAIBG (R/0482/2015).

LTAIBG-. Esta limitación afectaría a cualquier persona afectada por las actuaciones cualquiera que sea la posición que ocupe (informe IAI 5/2019).

Por otra parte, el carácter reservado o confidencial que tienen este tipo de actuaciones hace que los trabajadores que intervienen lo hagan confiando en que sea preservada su identidad.

Sin embargo, desde el punto de vista de la protección de datos personales nada impediría que se pudiera facilitar al solicitante una lista con el conjunto de actuaciones realizadas (omitiendo cualquier dato personal), a los efectos de que pueda comprobar si se ha actuado o no de conformidad con lo previsto en el Protocolo para estos casos.

Una vez concluidas las actuaciones previstas en el Protocolo, si se ostenta la condición de interesado, el solicitante tiene derecho a acceder a toda la información que sobre su persona figure en la información aportada o generada en el transcurso de estas. Sin embargo, el acceso a la identidad de los trabajadores que puedan haber facilitado información sobre el reclamante podría verse limitado en función de las circunstancias que puedan alegar estas personas respecto a esta cuestión (informe IAI 5/2019).

Con anterioridad a este pronunciamiento de la APDCat, el CTA ha puesto de relieve que “[...] el sigilo y la confidencialidad exigidos son principios necesarios y razonables teniendo en cuenta la naturaleza y sensibilidad de la información contenida en una denuncia de acoso laboral, por lo que deben mantenerse durante el transcurso de las actuaciones. La aplicación de estos principios garantiza que la Comisión pueda recabar la información necesaria para adoptar sus conclusiones; no obstante, una vez finalizadas éstas, no puede obviarse el derecho del denunciado a conocer el contenido de la denuncia”. Por ello, “[...] una vez finalizadas las actuaciones ante una denuncia de acoso laboral que establece el Protocolo, el denunciado tendrá derecho a acceder a ésta, previa omisión de aquellos datos que se refieran al estado de salud del denunciante” (R 1/2019).

10.5. ACCESO POR PARTE DE TERCEROS A DATOS DE PROCEDIMIENTOS DISCIPLINARIOS

A tenor de lo dispuesto en el artículo 15.1 LTAIBG, “si la información solicitada contuviera datos relativos a la comisión de infracciones penales o administrativas que no conllevaran la amonestación pública al infractor, el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley”. Debe entenderse que este mismo criterio ha de seguirse para las infracciones laborales.

No obstante, si de lo que se trata es de un posible conflicto entre el derecho a la libertad de información y el derecho a la protección de datos personales (supuestos de relevancia o notoriedad pública), se exige una cuidadosa ponderación de las circunstancias de todo orden que concurren en el concreto caso examinado, tal y como se señala en la STS núm. 7025/2011, de 19 de octubre) (RJ 2012/1296), por lo que no puede concluirse que deba denegarse la información en todo caso.

10.6. ACCESO POR PARTE DEL INTERESADO A DATOS DE PROCEDIMIENTOS DISCIPLINARIOS

Cuando se haya iniciado un procedimiento disciplinario, el inculpado tiene derecho a que se le dé traslado del expediente (como interesado en el mismo), una vez cumplimentadas las diligencias previstas en el Título II del Real Decreto 33/1986, con el objeto de que pueda alegar lo que estime pertinente a su defensa y aporte cuantos documentos considere de interés. Se facilitará copia completa del expediente al inculpado cuando éste así lo solicite.



No obstante lo anterior, no sería acorde con el principio de minimización la comunicación de datos personales que obren en el expediente cuyo conocimiento no sea relevante para el ejercicio del derecho de defensa del interesado.

10.7. TRATAMIENTO DE DATOS EN SISTEMAS DE INFORMACIÓN DE DENUNCIAS INTERNAS

En el caso de que la Universidad establezca un sistema de quejas o denuncias internas, los empleados y terceros deberán ser informados acerca de la existencia de estos sistemas.

El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan.

Sin perjuicio de la notificación a la autoridad competente de hechos constitutivos de ilícito penal o administrativo, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador, dicho acceso se permitirá al personal con funciones de gestión y control de recursos humanos.

Deberán adoptarse las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente la de la persona que hubiera puesto los hechos en conocimiento de la entidad, en caso de que se hubiera identificado.

Los datos de quien formule la comunicación y de los empleados y terceros deberán conservarse en el sistema de denuncias únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados.

En todo caso, transcurridos tres meses desde la introducción de los datos, deberá procederse a su supresión del sistema de denuncias, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica. Las denuncias a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 32 LOPDGDD.

Transcurrido el plazo mencionado en el párrafo anterior, los datos podrán seguir siendo tratados, por el órgano al que corresponda, conforme a lo indicado en los párrafos segundo y tercero, la investigación de los hechos denunciados, no conservándose en el propio sistema de información de denuncias internas -art. 24 LOPDGDD-.

11. PUBLICACIÓN DE DATOS PERSONALES

11.1. ASPECTOS GENERALES

Cuando sea obligatoria la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente. Cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse.

Sea de forma electrónica o en formato papel, se publicará el documento identificativo (documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente de los interesados) siguiendo la [Orientación para la aplicación provisional de la Disposición Adicional Séptima de la LO 3/2018](#), aprobada por la AEPD, salvo en aquellos supuestos en los que legalmente no se exija la publicación del número del documento identificativo, en cuyo caso se omitirá este dato personal, o exista una coincidencia de nombre y apellidos y, por tanto, estaría justificada la inclusión también del segundo elemento identificador.

La publicación deberá realizarse de manera que no suponga un acceso indiscriminado a la información. Se recomienda que se realice en la intranet de la Universidad (con acceso restringido a los interesados en el procedimiento en cuestión) y cuando sea obligatorio por la norma otro medio de publicación o no quede suficientemente garantizado el conocimiento del acto a través de su publicación en la intranet, se adoptarán las medidas indicadas en esta Guía para la [publicación en tableros físicos](#).

Cuando hayan transcurrido los plazos de posibles impugnaciones, hay que retirar los documentos publicados sin dilación, sin perjuicio de la conservación por la Unidad de la correspondiente documentación acreditativa.

No se debe publicar información que ponga de manifiesto una situación personal, familiar o social (capacidad económica, situación de riesgo de exclusión, o cualquier otra circunstancia similar), salvo que sea estrictamente necesaria para garantizar la transparencia de la actividad relacionada con el funcionamiento y control de la actuación pública o venga expresamente dispuesto en norma de rango legal, en cuyo se hará utilizando códigos o identificadores.



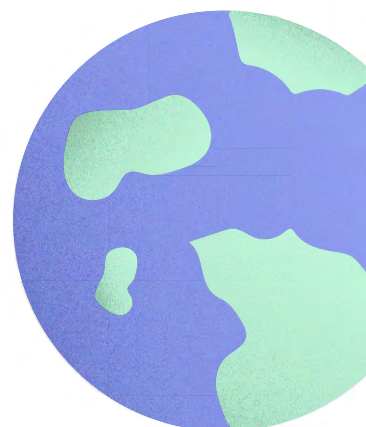
Buena práctica: la información que ponga de manifiesto una situación personal, familiar o social estará disponible en la respectiva Unidad para que los interesados puedan consultarla, en la medida en que sea estrictamente necesaria para la defensa de sus derechos e intereses.

Buena práctica: cuando la normativa específica de cada Universidad prevea la publicación en su página web en abierto, se aconseja facilitar la no indexación por los motores de búsqueda añadiendo los documentos al protocolo robots.txt.

11.2. PUBLICACIÓN DE DATOS PERSONALES RELATIVOS A PROCEDIMIENTOS DE SELECCIÓN DE PERSONAL

En los procedimientos selectivos, los principios de publicidad y transparencia son esenciales porque son la base de la igualdad, mérito y capacidad en el acceso a los puestos.

De hecho, numerosas leyes autonómicas de transparencia incluyen entre las obligaciones de publicidad activa la información relativa a los procesos de selección de personal.



Sin embargo, las obligaciones de transparencia en este tipo de procesos deben compatibilizarse con el derecho a la protección de datos personales, por lo que –como manifiesta la AEPD– la publicación en internet, primero, ha de estar prevista en la convocatoria y, segundo, preservándose que los accesos lo sean solo a los interesados (E-00110/2019).

En este sentido, la autoridad de control ha expresado su criterio en diversas resoluciones correspondientes a procedimientos sancionadores (por todas, AP/0017/2017; AP/0002/2017), llegando a afirmar lo siguiente:

- *“Publicidad/público es un término equívoco que no quiere decir publicación en la web de todo y de todos los trámites y que se relaciona con el principio de transparencia”.*
- *“Una vez publicada la convocatoria y las bases, los trámites siguientes van a afectar a un círculo específico y cualificado. La exposición de datos dentro de dicho círculo es adecuada, proporcionada y obedece a sus finalidades. Estas finalidades son las de los afectados por el procedimiento, para por ejemplo impugnar los actos que consideren son arbitrarios o lesionen sus intereses, así como para computar plazos de subsanaciones y/o reclamaciones”.*
- *“[...] el resto del público, los que no se someten a dichas pruebas, carecen de una base legítima para que puedan acceder a los datos de apellidos y nombre junto al NIF de cada aspirante o a sus calificaciones. Ello no es proporcionado con la finalidad del proceso, y no afecta a la transparencia, pues terceros que no se van a examinar, no concurren. Ese acceso por cualquier persona a los datos resulta invasivo, y es contrario al principio de minimización y calidad de datos en el tratamiento de los mismos”.*

Por ello, la AEPD advierte que *“las recomendaciones adecuadas para el tratamiento de los datos en forma de publicación en procesos selectivos ha de considerar:*

- En las bases de la convocatoria se ha de contener un apartado específico al tratamiento de datos y la tramitación del proceso para los aspirantes que podrán acceder todos ellos a los tramites provisionales del mismo mediante algún tipo de asignación de claves que se podrían generar en el momento de presentación de las solicitudes o combinándolo con otro dato de autenticación.*
- Por afectar a todos los aspirantes, todos deberán poder visionar la totalidad del listado con el resto de los datos de los aspirantes. En motivos de exclusión se deberán prever supuestos genéricos.*
- Información en el momento de acceder a las consultas por los afectados, que informe de las finalidades de la misma y advierta del estricto uso de las mismas, incurriendo en desvío de finalidad si el acceso a las consultas a los datos es para otra finalidad.*
- Minimización de datos”* [actualmente en el sentido previsto en la [Orientación para la aplicación provisional de la Disposición Adicional Séptima de la LO 3/2018](#)].

Posteriormente, la autoridad de control ha reiterado que la transparencia afecta exclusivamente a los admitidos o excluidos, deviniendo la exposición de datos desproporcionada cuando dichos datos resultan visibles para todo el mundo, pues no es necesario para la finalidad de publicidad y transparencia que estos lo conozcan (AP-00046/2018; AP/00010/2018).



Buena práctica: cuando en la convocatoria de un proceso de selección de personal –Ley del Concurso– se prevea la publicación de los actos en la página web de la Universidad, se debe abogar por la publicación restringida (intranet) a los participantes, siguiendo las recomendaciones de la AEPD citadas anteriormente.

11.3. PUBLICACIÓN DEL DATO DE DISCAPACIDAD EN LOS PROCESOS SELECTIVOS

La AEPD señala que debe evitarse la publicación referida a la condición de minusválido de aquellas personas que se presentan, sean admitidos o excluidos, al deducirse de la misma información sensible (AP-00054/2015)²⁶.

Por ello, se ha de evitar la publicación en internet en abierto de cualquier información de la que se infiera, directa o indirectamente, la condición de discapacitado de un aspirante, quedando restringido el acceso al simple conocimiento de la participación por el cupo de reserva para estas personas a los aspirantes de cada proceso selectivo.

11.4. VÍCTIMAS DE VIOLENCIA DE GÉNERO

La Disposición Adicional Séptima de la LOPDGDD establece que “*el Gobierno impulsará la elaboración de un protocolo de colaboración que defina procedimientos seguros de publicación y notificación de actos administrativos*”. No obstante, sin perjuicio de esta previsión de específico desarrollo reglamentario, las normas sobre medidas de protección integral de violencia de género establece que en actuaciones y procedimientos relacionados con la violencia de género se protegerá la intimidad de las víctimas; en especial, sus datos personales, los de sus descendientes y los de cualquier otra persona que esté bajo su guarda o custodia (art. 63.1 de la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género).

Por ello, se deberá actuar con especial cautela, utilizando cualquier medida de previa disociación de los datos personales de los que se pueda, explícita o implícita, inferirse la condición de víctima de violencia de género.



Buena práctica: incluir un código o identificador numérico que haga que la persona interesada -y solo ella- pueda identificarse.

11.5. AYUDAS PARA ESTUDIANTES CON NECESIDADES EDUCATIVAS ESPECIALES

Establece el artículo 5.3 LTAIBG, precepto que se reproduce en las leyes autonómicas en la materia, que “*cuando la información contuviera datos especialmente protegidos, la publicidad sólo se llevará a cabo previa disociación de los mismos*”. Por tanto, como afirma la AEPD, en este tipo de ayudas -que habitualmente contienen categorías especiales de datos- no se dará publicidad activa, de conformidad con la Ley de Transparencia, a ningún dato que permita identificar al interesado (ello incluye su nombre y/o apellidos, o el DNI, pasaporte o NIE etc.), se le haya concedido o desestimado la ayuda (informe 0240/2017). A mayor abundamiento, la Agencia incide en que la exposición de información a personas con este tipo de necesidades derivada de la discapacidad, o de trastornos graves de la conducta, debe ser muy estricta y no revelarse en principio más que a los interesados en el procedimiento, por lo que “*los fines de publicación son el conocimiento de los que participan en el proceso y esto se puede cumplir con la asignación de claves y contraseñas de los participantes para acceso exclusivo de los mismos*” (AP/00016/2017).

La propia normativa de subvenciones (Ley 38/2003) especifica que no serán publicadas las subvenciones concedidas cuando la publicación de los datos del beneficiario en razón del objeto de la subvención pueda ser contraria al respeto y salvaguarda del honor, a la intimidad personal o familiar de las personas físicas (art. 20.8.b).

En este sentido, la APDCat afirma que “*No hay suficiente habilitación legal, a los efectos del régimen de comunicación de datos para publicar y difundir el listado de las ayudas para alumnos con necesidad*

²⁶ En el caso en cuestión se había publicado en abierto en la página web del organismo.

específica de apoyo educativo, a menos que se preserve la identidad de los beneficiarios” (dictamen CNS 59/2016).

No obstante lo anterior, ello no será así respecto del importe de las ayudas de estas personas que sea posible separar de su condición de discapacidad si esta se constituye en la causante de la necesidad educativa especial, ya que sobre este importe, en las condiciones citadas, regiría el principio general de publicidad activa ya mencionado.

12. PERSONAL

12.1 PUBLICIDAD ACTIVA ²⁷

Entre otro tipo de información, se recomienda hacer pública la siguiente:

- Datos agregados sobre antigüedad de plantilla, incorporaciones por género, estructura por categorías profesionales
- Datos agregados sobre profesorado (por categorías, departamentos, centros, etc.)
- Datos agregados de PDI extranjero
- Datos agregados de personal investigador
- Retribuciones del personal que no dependan de situaciones individuales.
- Resultados de encuestas de satisfacción laboral
- Resultados agregados de la evaluación docente del PDI y de la evaluación del desempeño del PAS
- Breve currículum del PDI con acceso a información sobre su categoría profesional, cargos de gestión y resumen de la actividad académica e investigadora de los últimos cinco años
- Breve currículum de los miembros del equipo de gobierno y de los órganos unipersonales de gobierno
- Breve currículum de los puestos de libre designación a partir de nivel 28, según normativa autonómica
- Bandas salariales de PAS y PDI
- Asignación de docencia por áreas y departamentos
- Datos sobre evolución de la plantilla (promedio de edad, etc.)
- Claustro de docentes por estudios y asignaturas
- Datos agregados de perfil académico y formativo del personal de administración y servicios
- Tablas salariales según convenio colectivo
- Estadísticas sindicales (permisos sindicales, etc.)
- Datos agregados de horas extraordinarias realizadas
- Relación nominal de compatibilidades concedidas, en los términos previstos en la correspondiente normativa de transparencia

²⁷ Véase asimismo la [nota a pie 1](#) de la presente guía.

12.2. ACCESO A DATOS PERSONALES POR LOS REPRESENTANTES DE LOS TRABAJADORES

● Aspectos generales

Existe una doctrina consolidada que analiza la relación entre los derechos fundamentales a la libertad sindical y a la protección de datos que, en términos generales, aboga por la legitimidad del uso de aquella información necesaria y suficiente para que el órgano de representación pueda desempeñar con éxito las competencias que tiene reconocidas para la defensa, protección y promoción de los intereses de los trabajadores, sin que pueda exigirse de la empresa un deber de información más extenso o intenso que los previstos en las normas laborales y convencionales (por todas, *STS núm. 1387/1999*, de 2 de noviembre, FJ 4) (RJ 1999/9108).

Por consiguiente, como pone de manifiesto la ACPDCat, los representantes de los trabajadores pertenecientes a la representación sindical tienen derecho a acceder a los datos profesionales de los trabajadores en la medida en que esos datos sean necesarios para la negociación de las condiciones de trabajo de los trabajadores representados, para la emisión de informes, para informar a los trabajadores o bien para ejercer el control de legalidad. El acceso deberá realizarse anonimizando previamente los datos, excepto en el caso concreto de que el acceso a los datos personales sea necesario para cumplir su finalidad legítima y se ajuste a los principios establecidos en el art. 5.1 RGPD. En el resto de los casos, será necesario el consentimiento previo del afectado.

Los datos a los que tengan acceso los representantes de los trabajadores solo podrán destinarse al cumplimiento de las funciones en relación con las cuales una norma con rango de ley autoriza la cesión de dichos datos - art. 6.1.c) RGPD- y que estarán sometidos en su tratamiento por estos al deber de confidencialidad (*dictamen CNS 8/2008*).

En este sentido, la AEPD ha incidido de forma reiterada que la función de vigilancia y protección de las condiciones de trabajo, atribuida a las Juntas de Personal y los Comités de Empresa por el TRLEBEP y el TRLET, puede llevarse a adecuado desarrollo sin necesidad de proceder a una cesión masiva de los datos referentes al personal que presta sus servicios en el Órgano o Dependencia correspondiente. Solo en el supuesto en que la vigilancia o control se refieran a un sujeto concreto, que haya planteado la correspondiente queja ante el órgano de representación, será posible la cesión del dato específico de dicha persona. En los demás supuestos, la función de control quedará plenamente satisfecha mediante la cesión al órgano de representación de información debidamente dissociada, salvo que medie previo consentimiento de los afectados o la cesión se limite a las funciones asignadas a este tipo de órganos (por todos, informes *0091/2010*; *0079/2009*; *0118/2009*; *0632/2009*; *0437/2008*).

No obstante, podrían ampararse en el art. 6.1.b) RGPD las comunicaciones relativas a nóminas si el Convenio Colectivo de aplicación contempla la cesión de dicha relación, siempre que se atienda al principio de minimización y limitación de la finalidad (vigilancia del cumplimiento de las normas y pactos que regulan la relación laboral). De este modo, en la solicitud debe especificarse la necesidad concreta para la que se necesita tal información en relación con la citada vigilancia) (*informe 0384/2010*).

Atendiendo a las funciones de los órganos de representación de los trabajadores, como indica la AEPD, *“sí existe obligación de entregar los TC-1, boletín de cotización para la Seguridad Social en el que se reflejan los datos relativos a la identificación de la empresa y a la determinación de la deuda y el TC-2 en el que aparece reflejada la relación nominal de trabajadores y contiene los datos relativos a la identificación de los trabajadores, a sus bases de cotización y a las prestaciones que les hayan sido satisfechas en régimen de pago delegado”* (informes *0488/2009*; *0524/2008* y *0300/2008*).

Del mismo modo, los representantes de los trabajadores pertenecientes a la representación sindical tienen derecho a acceder a la copia básica de los contratos de trabajo realizados por esta empresa pública, copia que incluye los datos identificativos de los trabajadores excepto el DNI, el domicilio, el

estado civil y cualquier otro dato que, de acuerdo con la LO 1/1982, de 5 de mayo, pueda afectar a la intimidad personal de los afectados.

Con respecto al personal nombrado, los representantes de los trabajadores pertenecientes a la representación sindical tienen derecho a acceder a los datos de carácter personal identificativos de los trabajadores que consten en las resoluciones de nombramiento de éstos.

- *Acceso de los órganos de representación a expedientes de información reservada*

El acceso al número de expedientes de información reservada previa abiertos por la Universidad, los motivos por los que se han abierto, y respecto a los expedientes finalizados cuántos han sido archivados y cuántos han acabado con la incoación de un expediente disciplinario, no debería suponer, en principio, ningún inconveniente desde la perspectiva de la protección de datos de carácter personal, siempre que esta información se facilite de manera agregada y sin que sea posible identificar directa o indirectamente a los trabajadores objeto de estas investigaciones. Todo ello, sin perjuicio de que respecto a aquellas informaciones reservadas que aún estén en tramitación pueda concurrir el límite previsto en el artículo 14.1.e) LTAIBG o precepto equivalente de la ley de transparencia autonómica (dictamen CNS 14/2018).

- *Información a representantes de los trabajadores de sanciones disciplinarias*

Dado que el artículo 40.1.c) TRLEBEP establece, entre las funciones de los órganos de representación, ser informados de todas las sanciones impuestas por faltas muy graves, desde la perspectiva de la normativa de protección de datos de carácter personal no hay obstáculo para llevar a cabo esta comunicación, indicando el nombre y los apellidos de la persona sancionada y la sanción impuesta (dictamen CNS 5/2017).

- *Información al órgano de representación de los trabajadores de las ayudas individualizadas recibidas en concepto de acción social*

El conocimiento de los trabajadores que perciben las ayudas de acción social, así como su importe (que podría desvelar el acceso a datos personales que afectan a la intimidad, como el número de hijos, o el estado civil) no queda amparado en la LTAIBG (R/0462/2016).

- *Acceso a los datos de bajas laborales por los representantes de los trabajadores*

Si el parte de baja recoge datos de salud solo podrá ser comunicado cuando el afectado preste su previo consentimiento o concurra cualquiera de las otras bases de legitimación previstas en el art. 9.1 RGPD.

Del mismo modo, si no se pretende acceder al parte de baja, sino simplemente conocer el número de días de baja de un trabajador (considera la AEPD que el hecho de estar dado de alta o baja no es un dato de salud), teniendo en cuenta que entre las funciones contempladas en el TRLEBEP para los órganos de representación de los trabajadores no se contempla las comunicaciones relativas a las bajas de los trabajadores, sería necesario el previo consentimiento del afectado o la concurrencia de alguna de las causas de legitimación previstas en el art. 6.1 RGPD (informe 0009/2010).

- *Acceso a los datos de horas extraordinarias detalladas con nombre y apellidos del trabajador*

A raíz de la entrada en vigor del registro diario de jornada (12 de mayo de 2019), pueden darse dos situaciones:

Respecto al personal laboral, el nuevo apartado 9 del artículo 34 del TRLET, introducido mediante Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la

precariedad laboral en la jornada de trabajo, establece la obligación de que estos registros queden a disposición de los representantes de los trabajadores, por lo que existe en consecuencia habilitación legal expresa para que estos tengan acceso al registro de horas extraordinarias, y el acceso al registro incluiría también la identidad de las personas trabajadoras afectadas, según advierte la ACPDCat en su [informe IAI 27/2019](#).

Sin embargo, al circunscribirse la citada modificación legislativa al ámbito del personal laboral, teniendo en cuenta que en el TRLEBEP no hay una norma en idéntico sentido que permita a la institución comunicar la información relativa a las horas extraordinarias del personal funcionario de manera individualizada y que las reglas jurídicas en materia de protección de datos personales no admiten una interpretación extensiva, se recomienda, salvo que por las autoridades de control se indique lo contrario, que se recabe el consentimiento previo de los funcionarios, o bien facilitarla de manera anonimizada. En este sentido, sería una opción válida la posibilidad de emplear un código numérico para cada trabajador en sustitución de su nombre y apellidos, con la condición que se ofrecieran suficientes garantías de que no sería posible alcanzar identificar, ni directa ni indirectamente, estos trabajadores ([dictamen CNS 4/2013](#))²⁸.

- *Acceso por parte de los representantes de los trabajadores a los datos relacionados con la productividad abonada*

El CTBG se fundamenta en los criterios incluidos en el [dictamen conjunto de 24 de junio de 2015](#) para desestimar el acceso a la productividad nominal de los trabajadores por parte de representantes sindicales (R/0134/2016).

- *Comunicación a los representantes de los trabajadores de las direcciones de correos electrónicos profesionales de los trabajadores*

El Tribunal Constitucional (entre otras, [STC núm. 281/2005, de 7 de noviembre](#)) (RTC 2005\281), en su análisis del derecho fundamental a la libertad sindical, viene a señalar que el desarrollo legislativo del artículo 28.1 de la Constitución Española previsto en la Ley Orgánica 11/1985, de 2 de agosto, de Libertad Sindical, no agota las posibilidades de los sindicatos para difundir información sindical. Por ello, el citado derecho alcanza a la comunicación de las direcciones de correo electrónico profesional de los trabajadores a los representantes de los trabajadores y las organizaciones sindicales más representativas (por todos, informes AEPD [0347/2010](#); [0101/2008](#); [0658/2008](#); [resolución GAIP 331/2018](#)). Se estaría ante una cesión amparada en el cumplimiento de una obligación legal (amparo del derecho a la libertad sindical) sin perjuicio de aquellos casos excepcionales en los que deba prevalecer el derecho a la protección de datos. En ningún caso se comunicarán direcciones de correo privadas del trabajador, ni se podrá utilizar el dato en cuestión para fines distintos de la comunicación de información sindical de interés para los trabajadores.



Buena práctica: el uso de listas de distribución específicas para envío de información sindical, que deben permitir la baja en las mismas, salvo en los periodos electorales.

La delimitación de las responsabilidades y el ejercicio de derechos cuando los representantes de los trabajadores utilizan listas de distribución puestas a su disposición por la institución, ha sido objeto de la [SAN núm. 460/2016, de 28 de febrero de 2018](#) (JUR 2018\99453). El citado órgano judicial sostiene que la representación sindical respecto de los datos personales que figuran en las listas de distribución a las que envía la información sindical, no tiene la condición de responsable de tratamiento, ni tampoco

²⁸ En cualquiera de ambos casos, la ACPDCat extiende su criterio también a la información sobre las horas extraordinarias que no han sido pagadas, sino compensadas en horas.

le corresponde atender el derecho de oposición ejercido por el afectado al no tener “[...] acceso a las direcciones de correo que forman parte de las listas de distribución a las que envía la información sindical, ni mucho menos acceso a los datos personales de quienes figuran en tales listas de distribución, sino que únicamente conoce una dirección genérica (la de la lista de distribución) y no el nombre, apellidos, correo electrónico y categoría profesional de quienes integran las repetidas listas de distribución [...]” (FJ 7).

12.3. COMPATIBILIDADES

- *Acceso a autorizaciones o reconocimientos de compatibilidad*

Partiendo de la premisa de que se trata, al menos en lo que respecta a la LTAIBG, de una obligación de publicidad activa (art. 8.1.g), en los casos en que se haya autorizado o reconocido la compatibilidad de una actividad secundaria, la LTAIBG justificaría que, en atención al interés público prevalente, se permita el acceso a los datos meramente identificativos (nombre, apellidos y cargo) del empleado público afectado, así como la actividad y la empresa o entidad donde la desarrolla, salvo que la persona afectada se encuentre en una situación de protección especial, circunstancia que justificaría llevar a cabo una nueva ponderación (por todas, resolución del CTBG:R/0432/2016; resolución de la Comisión de Transparencia de Castilla y León: CT-0045/2016).

- *Publicación de autorizaciones de compatibilidad*

En los casos en que se haya autorizado la compatibilidad de un segundo puesto de trabajo, como subraya la APDCat, la LTAIBG habilitará la publicación del nombre y apellidos de la persona afectada, datos relativos al puesto de trabajo ocupado, datos de la actividad para la que se autoriza la compatibilidad, duración de la compatibilidad y demás condiciones a que esté sometida la compatibilidad. Desde el punto de vista de la normativa de protección de datos es preferible que esto no se lleve a cabo a través de una publicación directa de la resolución o autorización, sino a través de la publicación de un extracto de las mismas que contenga esta información, siempre atendiendo al principio de minimización de datos (dictamen CNS 51/2014).

12.4. ACCESO A DATOS RELATIVOS A LA SALUD LABORAL

- *Acceso a los datos de nombre y apellidos de los trabajadores que solicitan cambio de puesto por causas de salud*

Señala la APDCat que la comunicación de la información de carácter personal a los miembros del Comité de Seguridad y Salud podría realizarse sin el consentimiento expreso de los afectados, al entender que encuentra habilitación en las previsiones del artículo 39.2.c) de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales (en adelante, LPRL) (dictamen CNS 47/2014). En tal sentido, podrán acceder a los datos personales estrictamente necesarios sobre daños en la salud de los trabajadores que estén relacionados con el entorno laboral, solo para la finalidad de control que les atribuye la LPRL.

En cuanto al acceso de los delegados de prevención a los datos nominales de evaluación de adecuación a puesto estaría legitimada en virtud de lo previsto en el artículo 36 LPRL, dado el cumplimiento de una obligación legal por parte de la institución -art. 9.2.b) RGPD en relación con el art. 6.1.c)-, siempre que se atiende al principio de limitación de la finalidad y al principio de minimización. En tal sentido, podrán acceder a los datos personales estrictamente necesarios sobre daños en la salud de los trabajadores que estén relacionados con el entorno laboral, solo para la finalidad de control que les atribuye la LPRL.



- *Acceso a otros datos personales por parte de delegados de prevención y órganos de dirección de personal*

El tratamiento o cesión a los delegados de prevención del listado de personas incluidas como potencialmente expuestas a agentes susceptibles de causar daños graves a la salud de los trabajadores, incluidas las personas que ya no están vinculadas a la empresa, se ajustaría a la normativa de protección de datos, de acuerdo con los artículos 6.1 c) del RGPD y 22.1 y 5, 36.1 a) y 36.2 b) de la LPRL, y no requeriría el consentimiento de estas personas. Por ello, como sostiene la APDCat, el tratamiento o cesión a los delegados de prevención de los nombres y puestos de trabajo de las personas afectadas por la exposición a esos agentes se ajustaría a la normativa de protección de datos, de acuerdo con los artículos 9.2 b) y h) del RGPD y 22.4 y 36.2 c) de la LPRL, y no requeriría el consentimiento expreso de los afectados ([dictamen CNS 64/2018](#)).

Si lo que se pretende es el acceso al historial médico, como consecuencia de los reconocimientos médicos realizados a los trabajadores, deberá limitarse a las previsiones del artículo 22.4 de la LPRL (conclusiones que se deriven de los reconocimientos efectuados en relación con la aptitud del trabajador para el desempeño del puesto de trabajo o con la necesidad de introducir o mejorar las medidas de protección y prevención, a fin de que puedan desarrollar correctamente sus funciones en materia preventiva).

Por tanto, como pone de relieve la AEPD, será necesario el previo consentimiento del afectado para el acceso ajeno *“a los profesionales médicos evaluadores de la salud del trabajador, a la información contenida en la historia clínica determinante del pronunciamiento de la incapacidad o de la condición de apto o no para un determinado puesto de trabajo, que en aras del respeto al principio de la confidencialidad e intimidad del trabajador, no alcanzará al conjunto de pruebas clínicas que le hubieren practicado [...]”* ([informe 0240/2009](#)).

Por lo que respecta al acceso de los delegados de prevención a datos de accidentes de trabajo, teniendo en cuenta que el objeto de protección es el derecho a la salud tanto del trabajador accidentado como del resto de trabajadores de la empresa, puede entenderse que, en determinados casos, habrá que facilitar a los delegados de prevención información del parte de accidente de trabajo que resulte relevante para conocer las circunstancias en que se produjeron los daños a la salud del trabajador, para poder ejercer correctamente sus funciones en materia preventiva, establecidas en el art. 36.2.c) de la LPRL.

Así, con este fin, podría estar justificada la comunicación de los datos identificativos y de contacto del trabajador, la identificación de los posibles testigos del accidente de trabajo o, incluso, las del médico que efectúa la asistencia sanitaria que consten en el parte de accidente de trabajo.

No resultaría adecuada, por aplicación del principio de minimización, a juicio de la APDCat, la comunicación de los datos económicos del parte de accidente de trabajo, dado que se trata de información excesiva para el cumplimiento de la finalidad apuntada ([dictamen CNS 43/2014](#)).

12.5. ACCESO A DATOS DE NOMBRE Y APELLIDOS DE LAS PERSONAS QUE OCUPAN LOS PUESTOS DE LA RPT

Los datos de la relación o catálogo de puestos de trabajo que consistan únicamente en los datos que deban figurar en dicha relación o catálogo junto con el nombre y apellidos de la persona que ocupa dicho puesto no son más que datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano (art. 15.2 LTAIBG). Por tanto, como recuerda la AEPD, *“la regla general es favorable a la publicidad, a no ser que en el caso concreto deba prevalecer la protección de datos personales u otros derechos constitucionales. Para considerar si existe o no un caso concreto en el que deba prevalecer esta protección de otros derechos, antes de conceder el acceso a la representación unitaria de los trabajadores debería hacerse una notificación individualizada a todos los emplea-*



dos a los que se refiera la información, otorgándoles un plazo de quince días para que puedan formular alegaciones y oponerse, en su caso, al acceso previsto”. Por consiguiente, “deberán considerarse las circunstancias del caso concreto, para poder ponderar entre la prevalencia del derecho a la protección de datos o la transparencia en su vertiente de derecho de acceso. Sólo así se podrá valorar, por ejemplo, si la publicación pudiera afectar a su seguridad, como podría tratarse con víctimas de violencia de género [...]” que pueda resultar agravada por la divulgación de una información relativa al puesto de trabajo que ocupan (informe 0013/2016).

Anteriormente, el CTBG y la AEPD, en su [dictamen conjunto de 24 de junio de 2015](#), habían abogado por esta línea interpretativa, matizando que la información “no se facilitará cuando el acceso suponga un perjuicio para uno o varios de los bienes enumerados en el artículo 14.1 de la LTAIBG y la limitación sea justificada, proporcionada a su objeto y finalidad de protección y haya tenido en cuenta las circunstancias del caso concreto, especialmente la concurrencia en el mismo de un interés superior que justifique el acceso”; ni tampoco “cuando el acceso afecte a uno o varios empleados o funcionarios públicos que se encuentren en una situación de protección especial –p. ej. la de víctima de violencia de género o la de sujeto a una amenaza terrorista-, que pueda resultar agravada por la divulgación de la información relativa al puesto de trabajo que ocupan”.

A mayor abundamiento, en su [dictamen conjunto de 23 de marzo de 2015](#), ambos organismos ya habían expresado que “El criterio general favorable al acceso únicamente podría limitarse en caso de que en un caso concreto, en relación con un determinado empleado público y en atención a su situación específica, debiera prevalecer, conforme al apartado 2 del artículo 15 LTIPBG, la garantía de su derecho a la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación. Así, el acceso podría denegarse si el suministro de la información determinara de alguna manera la divulgación de datos de carácter personal en los términos del artículo 7 de la LOPD [actual art. 9.1 RGPD]”. Esta doctrina ha sido asumida por los organismos autonómicos de transparencia (por todas, resolución de la GAIP 263/2019).

12.6. ACCESO POR PARTE DEL PERSONAL A LAS CANTIDADES NOMINALES PERCIBIDAS EN CONCEPTO DE PRODUCTIVIDAD Y GRATIFICACIONES EXTRAORDINARIAS POR SUS COMPAÑEROS

En principio, no existiría impedimento para el acceso a las cantidades percibidas en concepto de gratificaciones y productividad por un empleado público que desempeñe un puesto de libre designación entre los niveles 28 y 30, así como el personal eventual y directivo, atendiendo a la relevancia de este perfil de puestos, salvo que atendiendo a las circunstancias concurrentes en un concreto caso deba prevalecer el derecho a la protección de datos. Respecto al resto de empleados, es públicamente relevante conocer la cantidad total abonada (por ejemplo por áreas) en concepto de gratificaciones. Al respecto, advierte el CTPDA que la difusión generalizada de dicha información, respecto de los empleados que no se encuentran entre los niveles mencionados *ut supra*, supondría un sacrificio excesivo de su privacidad (R 70/2018). En análogo sentido se pronuncia el CTA (R 31/2017).

Por su parte, la GAIP considera que el acceso a la información relativa al importe establecido para la gratificación por hora extraordinaria se puede hacer por para cada grupo y nivel de personal, funcionario o laboral, anonimizando (por ejemplo, mediante un código a cada persona) los importes retribuidos a cada perceptor de gratificaciones por horas extras, sin perjuicio que, en un caso futuro, la ponderación pueda ser eventualmente favorable al acceso no anonimizado, si se fundamenta en indicios de irregularidades que lo justifiquen (R 357/2017)²⁹.

El CTBG y la AEPD, en su [dictamen conjunto de 24 de junio de 2015](#), abogan por la aplicación para la productividad de los mismos criterios que para el acceso al conjunto de [retribuciones](#), reproducido en resoluciones posteriores del CTBG (por todas, resoluciones 0155/2019; 0460/2017; 0267/2016).

²⁹ El CTBG aboga por facilitar la información adicional, de carácter global y no individualizada, sobre los motivos y requisitos que se han debido de cumplir para ser merecedor de poder cobrar un complemento de “gratificación” (R/0053/2017).

Como precaución, y en caso de ser procedente el acceso, habrá que advertir que los datos se facilitan a “*periodo vencido, ya que el complemento de productividad no es un concepto fijo ni permanente y que está, en consecuencia, sujeto a incrementos y decrementos a lo largo del ejercicio presupuestario de forma individualizada. En todo caso, a falta de que se concrete otra cosa en la solicitud, la cantidad debería ser el bruto anual*” (dictamen conjunto CTBG y AEPD de 23 de marzo de 2015).

El CTBG aclara que la cantidad bruta anual se facilite, cuando se den las circunstancias contenidas en el dictamen conjunto citado anteriormente, sin desglose mensual. Tampoco se puede informar sobre el período en que se percibió el citado complemento, dado que los datos relativos a la salud –baja médica- se consideran especialmente protegidos y su acceso requiere el consentimiento de los afectados (RT 0140/2019).

12.7. DATOS PROFESIONALES DE CONTACTO

- *Solicitud de empresa externa de las direcciones de correos electrónicos profesionales de contacto del personal docente e investigador y de administración y servicios de la universidad con fines comerciales*

Los correos electrónicos profesionales se destinan a finalidades exclusivamente académicas o administrativas, por lo que no debe ser utilizado como medio de canalización de ofertas comerciales por parte de terceros.

Por tanto, se desestimará la solicitud por requerirse el previo consentimiento expreso de los interesados en aplicación del artículo 6.1.a) RGPD.

No obstante, se puede ofrecer –si la información es de interés general para el conjunto de trabajadores- la difusión del mensaje a través de un correo genérico de la institución

- *Publicación en el directorio de la Universidad de los datos de contacto del personal*

El tratamiento de los datos de contacto y, en su caso, los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica, siempre que se refieran únicamente a los datos necesarios para su localización profesional, y la finalidad sea la relación con la persona jurídica en la que prestan servicio, se fundamenta en el interés público –art. 6.1.e) RGPD y art. 19.3 de la LOPDGDD-.

No obstante lo anterior, atendiendo a la prevalencia del bien jurídico objeto de protección, deben estimarse sin dilación las solicitudes de ejercicio del derecho de oposición (art. 21.1 RGPD) por motivos relacionados con una situación particular debidamente acreditada (casos de violencia de género, amenazas terroristas, decisiones judiciales, etc.).



Buena práctica: incluir en la política de privacidad de la página web un aviso de que el tratamiento de los datos personales contenidos en el directorio sirve a fines exclusivamente académicos y administrativos sin que pueda ser utilizado por terceros para otros fines, entre ellos los comerciales, en cuyo caso sería puesto en conocimiento de la correspondiente autoridad de control el uso indebido en cuestión.

12.8. ACCESO A ESTUDIOS DE CARGA DE TRABAJO

No es información auxiliar o de apoyo aquella que es relevante en la conformación de la voluntad pública del órgano, como sería la distribución de efectivos destinados en un organismo. Este tipo de estudios estadísticos permite una gestión más eficiente de los recursos humanos identificando si la distribución de los efectivos existentes en cada momento se ajusta a la carga de trabajo, por lo que –como advierte el CTBG- se trata de documentación relevante para la toma de decisiones y que, por tanto, debe ser sometido al escrutinio de la acción pública (R/0540/2017).

13. ÓRGANOS DE GOBIERNO Y GESTIÓN INSTITUCIONAL

13.1 PUBLICIDAD ACTIVA ³⁰

- Órganos de gobierno de la Universidad
- Órganos unipersonales que colaboren con los órganos de gobierno de la Universidad
- Doctores *Honoris Causa*
- Redes institucionales de la Universidad
- Memorias de curso académico y de gestión
- Defensor Universitario.
- Delegado de Protección de Datos

13.2. ACCESO A DOCUMENTACIÓN DE ÓRGANOS COLEGIADOS

● *Acceso a actas*

Los sujetos obligados a cumplir con las normas de transparencia, entre los que se encuentran las universidades públicas, publicarán de forma periódica y actualizada la información cuyo conocimiento sea relevante para garantizar la transparencia de su actividad relacionada con el funcionamiento y control de la actuación pública (art. 5.1 LTAIBG).

Con carácter general, se estimará la petición, anonimizando los datos personales de personas físicas que no sean pertinentes (dicha “anonimización” no debe alcanzar datos personales que se limitan estrictamente a identificar a los miembros que conforman el órgano colegiado ya que estarían incluidos en el art. 15.2 LTAIBG), salvo que sea de aplicación alguno de los límites contenidos en el art. 14.1 LTAIBG, o en un caso concreto, a la vista de las circunstancias concurrentes y realizado el juicio de ponderación (art. 15 LTAIBG) deba prevalecer el derecho a la protección de datos de carácter personal.

Al respecto, el CTPDA entiende que “[...] el hecho de que los titulares de un interés legítimo puedan solicitar a los órganos colegiados que les sea expedida certificación de sus acuerdos (art. 17.7 Ley 40/2015) en modo alguno se opone al derecho que ostentan todos y cada uno de los ciudadanos de acceder a la información pública existente en los reiterados órganos. Entender lo contrario [...] supondría que el conocimiento de la actividad y el funcionamiento de la totalidad de los órganos colegiados incardinados en los organismos y entidades sujetos al ámbito de la LTPA quedaría excluido del marco normativo regulador de la transparencia y, en consecuencia, al margen del escrutinio de la opinión pública” (R 31/2017)³¹.

³⁰ Véase asimismo la nota a pie 1 de la presente guía.

³¹ En análogo sentido se pronuncia el CTBG (por todas R/0217/2017) y el Consejo de Transparencia de la Región de Murcia (R/037/16).



- *Acceso a acuerdos de sesiones de órganos colegiados de gobierno y de dirección*

Debe prevalecer su acceso, por ser de interés público, si bien aquellos datos personales que no son relevantes, o que su conocimiento resulte desproporcionado, se han de omitir (principio de minimización) (por todas, resolución de la Comisión de Transparencia de Castilla y León: CT-0042/2016)³².

Los datos personales que no sean meramente identificativos de los miembros del órgano personal serán anonimizados.

- *Acceso a la grabación de los órganos colegiados por parte de sus miembros*

Se estimaría la petición, al existir un interés legítimo –art. 6.1.f) RGPD- derivado de su condición de miembro del órgano colegiado, sin perjuicio de la “anonimización” de aquellos datos que no sean proporcionados (alusión a datos de domicilio personal, salud, o similares).

- *Acceso a la grabación de los órganos colegiados por parte de terceros*

Se requiere el previo consentimiento de los interesados, salvo que se acredite un interés legítimo, y que prevalezca sobre el derecho a la protección de datos de los afectados.



Buena práctica: en cualquiera de los supuestos indicados en este subepígrafe se debería advertir, cuando se facilite la información, que los datos personales a los que se acceden no podrán ser divulgados, reproducidos ni en todo ni en parte, ni transmitidos ni registrados por ningún sistema de recuperación de la información, sin el previo consentimiento de los interesados.

13.3. ACCESO A INFORMACIÓN SOBRE CONCURRENCIA O NO DE CAUSA DE ABSTENCIÓN DE MIEMBROS DE ÓRGANOS COLEGIADOS

Con carácter general, se estimará la petición, anonimizando los datos personales de personas físicas que no sean pertinentes (dicha “anonimización” no debe alcanzar datos personales que se limitan estrictamente a identificar a los miembros que conforman el órgano colegiado ya que estarían incluidos en el art. 15.2 LTAIBG), salvo que sea de aplicación alguno de los límites contenidos en el art. 14.1 LTAIBG o, en un caso concreto, a la vista de las circunstancias concurrentes y realizado el juicio de ponderación (art. 15.3 LTAIBG), deba prevalecer el derecho a la protección de datos de carácter personal.

13.4. ACCESO A LOS CURRÍCULOS DE LOS MIEMBROS DEL EQUIPO DE GOBIERNO, ASÍ COMO DE LOS ÓRGANOS DE GOBIERNO Y REPRESENTACIÓN DE FACULTADES, ESCUELAS, DEPARTAMENTOS E INSTITUTOS UNIVERSITARIOS DE INVESTIGACIÓN

El escrutinio público sobre el perfil curricular de las personas que ejercen la dirección de la institución debe prevalecer, con carácter general, sobre el derecho a la protección de datos, al ser una exigencia de responsabilidad hacia la ciudadanía, por lo que debe estimarse el acceso, si bien limitado a aquellos aspectos del currículum que determinen la trayectoria académica y profesional del responsable público (principio de minimización), salvo que, a la vista de las circunstancias concurrentes y realizado el juicio de ponderación (art. 15 LTAIBG), deba prevalecer el derecho a la protección de datos de carácter personal.

³² El CTBG aboga de igual modo por el acceso siempre que no exista causa alguna de inadmisión o límite con relación a los mismos (RT/0145/2017).

13.5. PUBLICACIÓN DE LOS DATOS IDENTIFICATIVOS E IMÁGENES DE LOS MIEMBROS DE LOS ÓRGANOS DE GOBIERNO UNIPERSONALES

El principio de transparencia y, por ello, el conocimiento de quienes son sus titulares para una correcta fiscalización de la gestión universitaria aboga por la citada publicación, al existir un interés público para ello, considerando que son miembros de órganos de gobierno universitarios.



Buena práctica: siempre que los medios técnicos de mantenimiento de calidad de los datos lo permitan se recomienda que se publiquen las imágenes de los miembros de los órganos colegiados de gobierno, con fundamento en el interés de los miembros de la comunidad universitaria en poder conocer a sus representantes.

13.6. PUBLICACIÓN DE LA INFORMACIÓN RELACIONADA CON EL TRABAJO DEL EQUIPO DE GOBIERNO

Las universidades deben publicar la información relativa a las funciones que desarrolla, incluidas las directrices, instrucciones, acuerdos, circulares o respuestas a consultas planteadas por los particulares u otros órganos en la medida en que supongan una interpretación del Derecho o tengan efectos jurídicos -art. 7.a) LTAIBG en relación con el art. 6-.

En el caso de que la consulta verse sobre las materias sobre las que se esté trabajando y sobre las cuales no se haya dictado o emitido ningún acuerdo o resolución, se considerarían actuaciones de trámite con información auxiliar y de apoyo y, por tanto, no son susceptibles de publicación ni de comunicación a terceros -art. 18.1.b) LTAIBG-³³.

13.7. PUBLICACIÓN DE LA AGENDA DE LOS MIEMBROS DEL EQUIPO DE GOBIERNO

Al respecto, interesa traer a colación la [Recomendación nº 1/2017, sobre información de las Agendas de los responsables públicos](#), en la que el Consejo de Transparencia y Buen Gobierno, establece que *“si bien es cierto que los contenidos de las agendas de los altos cargos no están, en principio, afectados por el principio de publicidad activa de los artículos 6 y siguientes de la LTAIBG -que obliga a publicar, de oficio, determinada información de carácter institucional, organizativa y de planificación, información de relevancia jurídica e información económica, presupuestaria o estadística-, no es menos cierto que dichas previsiones normativas constituyen un mínimo que puede desarrollarse con carácter voluntario por parte del organismo concernido o que debe sumarse a la publicidad activa por aplicación de lo dispuesto en el artículo 10.2 de la LTAIBG, que prevé la incorporación a las obligaciones de publicidad activa de aquella información ‘cuyo acceso se solicite con mayor frecuencia’”*.

Aunque el criterio contenido en esta Recomendación va dirigida a miembros del Gobierno, Secretarios de Estado y Altos Cargos de la Administración (los definidos en el artículo 1 de la Ley 3/2015, de 30 de marzo, reguladora del ejercicio de Alto Cargo de la Administración General del Estado), es razonable que, por analogía, se haga extensiva su aplicación a las universidades.

³³ Sin perjuicio de lo indicado en el criterio interpretativo del CTBG (006/2015), de 12 de noviembre de 2015, relativo a las causas de inadmisión de solicitudes de información: información de carácter auxiliar o de apoyo, puede consultarse la [R/591/2018](#) del citado órgano, donde se expone jurisprudencia al respecto.

Cuando las reuniones se celebren con personas físicas deberá ponderarse en cada caso la procedencia del otorgamiento del acceso atendiendo a la condición de dicha persona y la condición en que asiste a la reunión (persona experta, particular, etc.)³⁴, sin que sea posible establecer un criterio general de ponderación en estos casos ([dictamen conjunto CTBG-AEPD, de 5 de julio de 2016](#)).

En cualquier caso, el ámbito objetivo se extenderá solo a aquellas reuniones que tengan lugar en ejercicio de las funciones públicas que tienen conferidas y en su condición de responsable público. Es decir, se excluye las que se realicen a título privado y no afecten a sus competencias.

En caso de que la información pudiera contener datos personales especialmente protegidos, en particular en atención a la naturaleza de las entidades participantes en la reunión, habrá de estarse a las reglas previstas en el artículo 15.1 LTAIBG.



Buena práctica: en aras de facilitar el adecuado conocimiento de la actividad pública de los responsables universitarios, se recomienda facilitar el acceso a las citadas agendas, siempre que la solicitud se refiriese expresamente a la identificación de los participantes en las reuniones con sus nombres y apellidos (autoridades públicas externas y cargos públicos universitarios). De haber en la reunión alguna otra persona que no entre de estas categorías se limitará a indicarse respecto a estas el Órgano, Organismo o Departamento en que los participantes presten sus servicios.

13.8. ACCESO A INFORME JURÍDICO

Concurriría la causa de inadmisión prevista en el art. 18.1.b) LTAIBG (información auxiliar o de apoyo) si el informe solicitado se inscribe dentro de las consultas habituales que realizan los órganos de gobierno. Distinto sería si se trata de un informe preceptivo dentro de un procedimiento, o que sirva de fundamento para la adopción de una decisión universitaria, tal y como señala el CTBG ([RT 0372/2018](#)) o el CTA ([R 11/2018](#); [R/28/2017](#))

Hay que recordar al respecto que la publicación de los informes con trascendencia jurídica en la esfera de derechos de los ciudadanos debe ser realizada de oficio, es decir, sin necesidad de previa petición de acceso, en aplicación del principio de publicidad activa.

³⁴ La GAIP indica diversos supuestos en su [resolución 151/2018](#).

03



Anexo I. Glosario

“Anonimización”

Es la disociación definitiva e irreversible de los datos personales.

Categorías especiales de datos personales

Se trata de aquellos datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. En concreto, lo son los que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

Comunicación o cesión de datos

Es el tratamiento de datos que supone su revelación a una persona distinta del interesado, excepto el acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable siempre que se cumpla lo establecido en el RGPD, la LOPDGDD y sus normas de desarrollo.

Consentimiento

En aquellos supuestos en los que la base jurídica del tratamiento sea el consentimiento, la citada manifestación de voluntad ha de prestarse de forma libre, específica, informada e inequívoca por la que se acepte, mediante una declaración o clara acción afirmativa, el tratamiento de datos que le conciernan al que lo presta. Una de las vías de acreditarlo puede ser mediante la marcación registrada de una casilla de verificación. En cualquier caso, el tratamiento estará limitado a la finalidad para la que se solicita el mismo -art. 5.1.b RGPD-.

Datos agregados

Ver “anonimización”.

Datos biométricos

Son los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

Datos especialmente protegidos

La LTAIBG califica como datos especialmente protegidos, a los efectos previstos en la citada norma, a las mismas categorías especiales de datos personales que posteriormente ha contemplado el RGPD con el añadido de los datos personales relativos a la comisión de infracciones penales o administrativas que no conlleven la amonestación pública al infractor.

Datos genéticos

Son los datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

Datos personales

Toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Datos relativos a la salud

Son los datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.



Deber de confidencialidad

Todas las personas que intervengan en cualquier operación de tratamiento están sujetas al principio de integridad y confidencialidad establecido en el art. 5.1.f) RGPD, con independencia del deber de secreto profesional que se le exija de conformidad con la legislación aplicable.

Ambas obligaciones se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

Destinatario

Es la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros.

Información de carácter auxiliar o de apoyo

No existe una definición nominal de lo que es información de carácter auxiliar o de apoyo a los efectos previstos en la legislación de transparencia. El artículo 18.1.b) de la LTAIBG ofrece una relación de documentos, a título ejemplificativo, que puede contener información con los condicionantes para ser calificada de carácter auxiliar o de apoyo, si bien será el contenido y no su formato o denominación la que determine si se está ante este tipo de información.

Interesado

Es la persona física titular de los datos personales.

Interés público

En cuanto al acceso a la información pública, con carácter general, habrá que entender que, en la medida en que este contribuya a un mejor conocimiento de los criterios de organización y funcionamiento de las instituciones o a la asignación de los recursos, cabrá considerar –con carácter general- la existencia de un interés público prevalente sobre los derechos a la protección de datos y a la intimidad en los términos y con las excepcio-

nes establecidas por la LTAIBG. Por el contrario, cuando la información no contribuya a un mayor conocimiento de la organización y funcionamiento de las instituciones o de la asignación de los recursos públicos, prevalecerá el respeto a los derechos a la protección de datos o la intimidad.

Juicio de ponderación

Se ha de valorar si existe un interés público o privado que prevalezca sobre el bien jurídico que justifica la limitación al acceso a la información pública. Se trata de ponderar entre los derechos e intereses favorables y opuestos al acceso. Para este ejercicio se atenderá, entre otros, a los criterios expuestos en el art. 15.3 LTAIBG, sin olvidar aquellos que puedan ser decisivos para la decisión final a adoptar (relevancia pública del titular de los datos, titularidad de un interés legítimo, una hipotética motivación de la solicitud aun no siendo obligatoria, la proporcionalidad, etc.).

Minimización de datos

La cesión o comunicación de datos personales, cuando exista base jurídica para ello, debe limitarse a aquellos que sean adecuados, pertinentes y estrictamente necesarios para la finalidad pretendida.

Obligaciones del cesionario

Cuando se revelan o comunican datos personales a terceros, estos quedan sujetos a la normativa de protección de datos personales y a los efectos legales que de ella se deriven en el tratamiento de datos que realice, sin que puedan tratar los datos personales para finalidades distintas para las que se le autorizó la comunicación.

Publicidad activa

Las Universidades públicas publicarán de forma periódica y actualizada la información cuyo conocimiento sea relevante para garantizar la transparencia de su actividad relacionada con el funcionamiento y control de la actuación pública. Podrá ser objeto de publicidad activa la información asociada o anonimizada (aquella que no guarde relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos

de forma que el interesado no sea identificable, o deje de serlo), sin perjuicio de aquella información que contenga datos personales en la medida en que se establezca expresamente su publicidad en virtud de lo previsto en la ley de transparencia aplicable en cada caso, o dicha publicidad venga establecida en la legislación sectorial correspondiente.

Reelaboración

Debe entenderse aplicable cuando: a) la información solicitada deba elaborarse expresamente para dar una respuesta, haciendo uso de diversas fuentes de información, o b) cuando el organismo o entidad carezca de los medios técnicos que sean necesarios para extraer y explotar la información concreta que se solicita, resultando imposible proporcionar la información solicitada.

“Seudonimización”

Es 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 garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

Tercero

Persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

Test del daño

Previamente a la ponderación establecida en el art. 15.3 LTAIBG, es necesario valorar si el acceso solicitado supone efectivamente un perjuicio y no meramente una simple afectación, a los derechos o intereses protegidos por el límite o límites concurrentes de los enunciados en el art. 14.1 de la citada norma legal, teniendo en cuenta que la aplicación de los meritados límites debe ser justificada y proporcionada al objeto y finalidad del bien jurídico que se trata de proteger.

Tratamiento

Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.



04



Anexo II. Lista de abreviaturas

**AEPD**

Agencia Española de Protección de Datos.

APDCat

Autoridad Catalana de Protección de Datos.

AVPD

Agencia Vasca de Protección de Datos.

ANECA

Agencia Nacional de Evaluación de la Calidad y Acreditación.

CC

Código Civil.

CTA

Consejo de Transparencia de Aragón.

CTBG

Consejo de Transparencia y Buen Gobierno.

CTN

Consejo de Transparencia de Navarra.

CTPDA

Consejo de Transparencia y Protección de Datos de Andalucía.

GAIP

Comisión de Garantía del Derecho de Acceso a la Información Pública.

LOPDGDD

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

LOREG

Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General.

LOU

Ley Orgánica 6/2011, de 21 de diciembre, de Universidades.

LPACAP

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

LPHE

Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español.

LPRL

Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.

LTAIBG

Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

PAS

Personal de administración y servicios.

PDI

Personal docente e investigador.

RD

Real Decreto

RGPD

Reglamento General de Protección de Datos, 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 y por el que se deroga la Directiva 95/46/CE.

SAN

Sentencia de la Audiencia Nacional.

SJSO

Sentencia del Juzgado de lo Social.

STC

Sentencia del Tribunal Constitucional.

STEDH

Sentencia del Tribunal Europeo de Derechos Humanos.

STJUE

Sentencia del Tribunal de Justicia de la Unión Europea

STS

Sentencia del Tribunal Supremo.

TRLEBEP

Real Decreto Legislativo 5/2015, de 5 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.

TRLET

Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

05



Anexo III. Documentación de interés

DIRECTRICES, DICTÁMENES Y DOCUMENTOS DEL GRUPO DE TRABAJO DEL ARTÍCULO 29

- Directrices del Grupo de Trabajo del Artículo 29 (WP 260) sobre el principio de transparencia regulado en el RGPD.
- Directrices del Grupo de Trabajo del Artículo 29 (WP 259) sobre el consentimiento regulado en el RGPD.
- Dictamen 02/2016, del Grupo de Trabajo del Artículo (WP 239), relativo a datos personales para fines de transparencia en el sector público.
- Dictamen 06/2014, del Grupo de Trabajo del Artículo 29 (WP 217), relativo al concepto de interés legítimo.
- Dictamen 05/2014, del Grupo de Trabajo del Artículo 29 (WP 216), relativo a técnicas de anonimización.
- Dictamen 01/2014, del Grupo de Trabajo del Artículo 29 (WP 211), relativo a la aplicación de los conceptos de necesidad y proporcionalidad.
- Dictamen 03/2012, del Grupo de Trabajo del Artículo 29 (WP 193), relativo al desarrollo de las tecnologías biométricas.
- Dictamen 15/2011, del Grupo de Trabajo del Artículo 29 (WP 187), relativo a la definición de consentimiento.
- Dictamen 04/2007, del Grupo de Trabajo del Artículo 29 (WP 136), relativo al concepto de dato personal.
- Documento de trabajo del Grupo del Artículo 29 (WP 104), relativo a la relación entre protección de datos y derecho de propiedad intelectual.
- Documento de trabajo del Grupo del Artículo 29 (WP 67), relativo a videovigilancia.
- Documento de trabajo del Grupo del Artículo 29 (WP 55), relativo a la vigilancia de las comunicaciones electrónicas en el trabajo.
- Dictamen 8/2001, del Grupo del Artículo 29 (WP 48), relativo al tratamiento de datos personales en el contexto del trabajo.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

- Nota técnica “La K-anonimidad como medida de la privacidad”.
- Orientaciones y garantías en los procedimientos de anonimización de datos personales.
- Guía sobre el uso de videocámaras para seguridad y otras finalidades.
- Orientación para la aplicación provisional de la Disposición Adicional Séptima de la LO 3/2018.

CRITERIOS DEL CONSEJO DE TRANSPARENCIA Y BUEN GOBIERNO³⁶

- Criterio interpretativo del CTBG (003/2016), de 14 de julio de 2016, relativo a las causas de inadmisión de solicitudes de información: solicitud de información repetitiva o abusiva.

³⁶ Disponibles en https://www.consejodetransparencia.es/ct_Home/Actividad/criterios.html



- Criterio interpretativo del CTBG (009/2015), de 12 de noviembre de 2015, relativo a la aplicación de la disposición adicional primera de la Ley 19/2013 sobre regulaciones especiales del derecho de acceso a la información pública.
- Criterio interpretativo del CTBG (008/2015), de 12 de noviembre de 2015, relativo a la actuación del órgano o unidad competente cuando, en el ejercicio del derecho de acceso, se solicite por los interesados información ya objeto de publicidad activa por el organismo de que se trate.
- Criterio interpretativo del CTBG (007/2015), de 12 de noviembre de 2015, relativo a las causas de inadmisión de solicitudes de información: relativas a información para cuya divulgación sea necesaria una acción previa de reelaboración (artículo 18.1.c de la Ley 19/2013).
- Criterio interpretativo del CTBG (006/2015), de 12 de noviembre de 2015, relativo a las causas de inadmisión de solicitudes de información: información de carácter auxiliar o de apoyo.
- Criterio interpretativo del CTBG (004/2015), de 23 de julio de 2015, relativo a la publicidad activa de los datos del DNI y de la firma manuscrita.

CRITERIOS CONJUNTOS DEL CONSEJO DE TRANSPARENCIA Y BUEN GOBIERNO Y DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS³⁷

- Criterio interpretativo conjunto del CTBG y de la AEPD (002/2016), de 5 de julio de 2016, sobre la información relativa a las agendas de los responsables públicos.
- Criterio interpretativo conjunto del CTBG y de la AEPD (002/2015), de 24 de junio de 2015, relativo a la aplicación de los límites al derecho de acceso a la información.
- Criterio interpretativo conjunto del CTBG y de la AEPD (001/2015), de 24 de junio de 2015, relativo al alcance de las obligaciones de los órganos, organismos y entidades del sector público estatal en materia de acceso a la información pública sobre sus Relaciones de Puestos de Trabajo (RPT), catálogos, plantillas orgánicas, etc.. y las retribuciones de sus empleados o funcionarios.

³⁷ Disponibles en https://www.consejodetransparencia.es/ct_Home/Actividad/criterios.html

