- Expediente N.º: EXP202200367

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes:

HECHOS

PRIMERO: Entre los días 10 de diciembre de 2021 y 9 de marzo de 2022, se recibieron en la Agencia Española de Protección de Datos, las reclamaciones remitidas por la ASOCIACIÓN DE ESTUDIANTES UNIR y 11 personas y asociaciones referenciadas en el Anexo 0. Las reclamaciones se dirigen contra la UNIVERSIDAD INTERNACIONAL DE LA RIOJA con NIF A26430439 (en adelante, la parte reclamada o UNIR). Los motivos en que basa la reclamación son los siguientes:

Se denuncian ciertos aspectos del tratamiento de datos personales que lleva a cabo UNIR, con la finalidad de confirmar la identidad de los alumnos que van a realizar los exámenes de forma telemática para prevenir el contagio de la Covid-19. Dicho tratamiento se realiza mediante una herramienta informática que los alumnos deben instalarse en su equipo, proporcionada por el proveedor SMOWL (la herramienta se llama SMOWLTECH). Esta aplicación hace uso de la cámara web frontal para registrar la imagen del estudiante mientras realiza su examen, y también captura las acciones que realizaban en el escritorio, con el teclado y el ratón. La herramienta también comprende la utilización de algoritmos de reconocimiento facial para determinar si la persona que se había inscrito en la prueba y había aportado su documento identificativo era, efectivamente, la que estaba realizándola. En el marco del procedimiento E/08977/2021, la universidad aseguró que no volvería a hacer uso de los mencionados algoritmos de reconocimiento facial, y pasaría a sustituirlos por un proceso de revisión manual realizado por personal del centro.

Aunque, dicho tratamiento facial ya fue objeto de reclamaciones pasadas, interpuestas ante la Agencia por algunos de los afectados, en los escritos recibidos en esta ocasión se denuncia una novedad presentada por la universidad para la convocatoria correspondiente a febrero de 2022. Según exponen los reclamantes, se ha incorporado el requisito obligatorio de que los alumnos examinados instalen una segunda cámara, además de la frontal que ya se venía utilizando, obligando a que dicha cámara enfoque el entorno del alumno, y se visualicen sus dos manos, su cuerpo y sus pantallas de trabajo, de forma que se vea claramente lo que está haciendo. De no hacerlo así, y según se denuncia, el estudiante obtendrá la calificación de cero en el examen, pudiendo motivar la pérdida de la evaluación continua.

Los afectados consideran que esta práctica no es proporcionada e intrusiva, y no respeta los derechos de los alumnos a la protección de sus datos o su intimidad (ni la de los familiares que sean grabados en el transcurso de la prueba). Algunos han citado o adjuntado la contestación de esta Agencia a una consulta sobre la utilización de tecnologías de vigilancia del entorno del alumno ("revisión 360º"), y otros adjuntan

copia de la resolución de la Universidad de Granada, de 4 de mayo de 2020, en contra del requerimiento de la segunda cámara para la evaluación. Una de las profesoras de la Universidad ha transmitido a una afectada la información de que habría sido la ANECA (Agencia Nacional de Evaluación de la Calidad y Acreditación) la que habría autorizado o dado su visto bueno al requerimiento.

Algunos afectados también cuestionan que un consentimiento a tal tratamiento de datos, así recabado, sea realmente libre, ya que los alumnos con un perfil de riesgo no tienen la opción de realizar el examen de forma presencial. Por tanto, el consentimiento no sería una base legal válida para el mismo. Otros inciden en que la universidad tampoco cuenta con una base de legitimación para obligar a sus alumnos a instalar un "software" que permite el acceso a sus equipos, donde se encuentra su agenda, aplicaciones bancarias, mensajes privados, contraseñas, etc.

Del análisis detallado de cada una de las reclamaciones recibidas cabe destacar:

- *En la **Reclamación 1** se aporta el "Manual De Estudiantes – Exámenes" elaborado por UNIR con las instrucciones para poder realizar el examen online, distribuidas entre los alumnos y con el detalle sobre el funcionamiento de las aplicaciones a instalar y los requisitos técnicos a cumplir.*

- *En la **Reclamación 2** se aporta una noticia publicada en prensa con el titular "La UGR prohíbe a los profesores pedir a los estudiantes dos cámaras en los exámenes online" (https://www.ideal.es/miugr/prohibe-profesores-pedir-camaras-estudiantes-20210118122657-nt.html). En ella se afirma que la UGR dictó resolución en mayo de 2020 prohibiendo el proctoring y regulando como proceder en videoconferencias. Tras consultar esta resolución se deduce que:*
  - *i. La UGR prohíbe el uso de herramientas de proctoring en la evaluación no presencial, no permitiéndose el uso de técnicas biométricas o de reconocimiento facial.*
  - *ii. La identificación del alumnado se realiza a través de la exhibición del DNI o cualquier otro documento válido.*
  - *iii. Las pruebas orales se graban para garantizar el derecho de revisión por el tiempo estrictamente necesario.*
  - *iv. Se utilizan sistemas de videoconferencia para el correcto desarrollo de la prueba, seguimiento e identificación del estudiantado. En este caso no es necesaria la grabación. Se indica que la videoconferencia no implica una vulneración de la intimidad personal o intromisión domiciliaria, en el bien entendido juicio de proporcionalidad que garantice tales derechos frente a las necesidades de interés público de la verificación del aprendizaje del estudiantado. El profesorado debe avisar al estudiantado para que organice el desarrollo de la prueba de forma que no interfiera en su ámbito exclusivamente doméstico.*

- *En la **Reclamación 3** se denuncia que la UNIR no está respetando la resolución de 27 de julio sobre el uso de técnicas biométricas y reconocimiento facial, también se denuncia la intrusión existente al exigir el uso de un dispositivo del propio estudiantado para activar la segunda cámara de vigilancia suponiendo esto una vulneración del derecho a la intimidad al*

poder provocar el uso de este dispositivo una brecha de filtración de datos personales almacenados en dispositivo.

- *En las **Reclamación 4, Reclamación 5 y Reclamación 6** también se denuncia la invasión de la intimidad que puede provocar el uso de la segunda cámara de seguridad utilizando un dispositivo propio del estudiantado, y la grabación del espacio doméstico del alumnado durante todo el tiempo del examen, vulnerando esto el derecho a la intimidad.*

- *En la **Reclamación 7** se denuncia lo siguiente:*
  - *i. Que en la matrícula que el alumno firma al inicio de curso únicamente se especifica lo siguiente: "los estudiantes deben disponer de una cámara web y audio para poder realizar adecuadamente las defensas de los trabajos fin de grado y fin de máster en línea", pero nunca se especifica nada sobre la existencia de la segunda cámara y la necesidad de utilizar un segundo dispositivo propio del alumnado.*
  - *ii. Se aporta en esta reclamación un anexo con el documento enviado por la UNIR a los alumnos sobre las recomendaciones y pautas a seguir para la correcta realización de los exámenes online, del análisis de este anexo se extrae:*
    - *a) Recomiendan desactivar el antivirus para evitar que se bloquee el programa de monitorización.*
    - *b) Indican que la prueba debe realizarse en una instancia cerrada. El estudiante debe encontrarse solo en la habitación. La cámara frontal debe enfocar al estudiante y la puerta de acceso en la medida de las posibilidades. El estudiante es el garante de que no habrá interrupciones de otras personas. En caso de alteración de las condiciones del entorno, el profesorado valorará el impacto en la evaluación.*
    - *c) En todo momento se mantendrá activa la monitorización del escritorio, las cámaras y el micrófono. La desactivación, desconexión o desenfoque o pérdida de visibilidad significativa podrá desencadenar una incidencia o alerta. Durante el examen es obligatorio:*
      - *Tener en todo momento activa la monitorización del escritorio.*
      - *Mantener las dos cámaras activas durante todo el examen y colocadas de forma que el estudiante pueda ser visto e identificado.*
    - *d) El dispositivo utilizado como segunda cámara debe tener conexión a internet y enfocar el entorno, siendo visibles las dos manos, el cuerpo y la pantalla de trabajo. Se aportan en este documento algunas imágenes ejemplo de lo que se debe recoger por la segunda cámara.*
  - *iii. Se aporta también en esta reclamación otro anexo con una comunicación enviada por el rector de la UNIR a todos los estudiantes en relación con las modalidades de realización de exámenes, del análisis de este documento se extraen los siguientes párrafos:*

a) *"Para la modalidad en línea se utilizarán sistemas de apoyo a la supervisión que han sido elegidos tras asegurar el cumplimiento de todos los requerimientos del RGPD, Ley 3/2018, y previa verificación exhaustiva del cumplimiento de las recomendaciones de la AEPD. Toda la documentación jurídica que avala esta decisión está a disposición de cualquier estudiante:*
   - *Análisis de los pronunciamientos y recomendaciones de distintas autoridades de control en materia de protección de datos.*
   - *Juicio de proporcionalidad constitucional.*
   - *Evaluación de impacto y análisis de riesgos.*
   - *Garantía contractual de la privacidad de los datos de los alumnos.*
   - *Garantía del principio de información."*

b) *"El sistema de apoyo a la supervisión capta imágenes y sonido del estudiante y entorno, pero no accede a ninguna información de su equipo informático, salvo que se muestre en la propia pantalla."*

c) *"Los estudiantes pueden optar por la modalidad que mejor se adapte a su situación personal y particular (presencial y online). Ambas modalidades se desarrollan dentro del respeto del marco legal y constitucional y ambas garantizan un sistema de evaluación eficaz y riguroso acorde con el prestigio académico de nuestra institución y el de los títulos que expedimos."*

iv. *Se aporta también en esta reclamación un anexo con la respuesta enviada por la Subdirección General de Promociones y Autorizaciones a una consulta planteada por esta misma RECLAMANTE, y con número de registro de entrada O00007128e21000XXXX. Del análisis de esta respuesta se destaca el siguiente párrafo:*

a) *" Así mismo y respondiendo a su preocupación por si la vigilancia del entorno del alumno o revisión 360 del domicilio en el que se realiza la prueba podría ser desproporcionada, dado que en el domicilio pueden convivir terceras personas o mostrarse elementos personales ajenos al objetivo de la propia prueba de evaluación y que podrían proporcionar información acerca de la intimidad del alumno o de terceros, podría entenderse como una injerencia en la propia intimidad del alumno y los posibles moradores del domicilio y, por tanto, un riesgo para el derecho a la intimidad y la inviolabilidad del domicilio del alumno".*

- *En la **Reclamación 8, Reclamación 9 Y Reclamación 10** se vuelve a denunciar la obligatoriedad del uso de la segunda cámara para los exámenes de la convocatoria de febrero de 2022, utilizando un dispositivo personal del propio alumno, provocando ello la posibilidad de acceso a la información personal contenida en el mismo.*

- *En la **Reclamación 11**, la "Asociación de Estudiantes X la defensa de los derechos fundamentales (HUXIR)" denuncia:*

i. *Que la UNIR ha hecho caso omiso de la resolución de advertencia firmada por la directora de la AEPD en 27 de julio de 2021 en relación con el uso de reconocimiento facial.*
ii. *Que los exámenes que se estaban realizando en el momento de poner la reclamación estaban haciendo uso de la segunda cámara a través de un QR no auditado y que podría exponer datos sensibles como fotos, cuentas bancarias…etc.*
iii. *Aportan captura de pantalla de una tutoría explicativa que se llevó a cabo el 22 de diciembre de 2021, sobre los exámenes a realizar y en la que se aprecia la siguiente frase en una de las diapositivas mostradas: "El dato biométrico se elimina una vez se cierran las actas y se elevan a definitivas".*
iv. *Se aporta email enviado por esta asociación (HUXIR) a la Oficina del Defensor Universitario, solicitando que medie para que inste a la UNIR a suspender el uso de la segunda cámara para las convocatorias de enero y febrero de 2022 puesto que no existe marco legal amparado por la AEPD.*

- *En la **Reclamación 12** se denuncia, por parte de un estudiante de la UNIR, la vulneración de sus derechos en los exámenes celebrados en convocatoria de febrero 2022 al violarse lo indicado en el informe de la AEPD 0036/2020 así como también la resolución del expediente E/05454/2021. Denuncia que la UNIR ha vuelto a realizar control biométrico en los exámenes de febrero de 2022.*
  i. *Que, en el proceso de registro para la realización de los exámenes online, en los términos y condiciones que el alumno debía aceptar (de forma previa al registro), se indicaba textualmente lo siguiente: "obtención a través de las imágenes y de los audios de un modelo biométrico de las características del usuario/a para poder realizar la identificación y comprobaciones posteriores sobre la identidad del usuario/a".*
  ii. *Que durante el proceso de registro se toman fotografías tanto de cara como de DNI.*
  iii. *Que la base jurídica para el tratamiento de los datos personales, en relación con el uso de la segunda cámara, se basa en el consentimiento y que este no puede ser otorgado libremente.*
  iv. *Aporta capturas de pantalla de lo anteriormente afirmado.*

- *En la de la asociación HUXIR vuelve a denunciar que UNIR hace caso omiso de la resolución de la directora de la AEPD de julio de 2021 al exigir el uso de una segunda cámara para los exámenes de enero a marzo, y solicitan a la AEPD que se interceda en su nombre ante UNIR. También se denuncia que en fecha 02 de febrero de 2022 se ejerció, por parte de un miembro de la asociación, los derechos de acceso a sus datos personales ante el responsable de tratamiento y que a fecha de entrada de la presente reclamación no había sido contestada.*

- *Por último, destacar también la recepción, en 13 de mayo de 2022, de un escrito enviado (…), comunicando a la AEPD la situación de indefensión jurídica en la que se encontraban por las acciones emprendidas por la otra*

asociación HUXIR, Asociación no reconocida por el alumnado UNIR y que según indican solo estaba respaldada por unos 10 estudiantes. En este escrito se manifiestan a favor de la UNIR indicando que la misma ha establecido un sistema de evaluación que garantiza la calidad y la fiabilidad de la prueba, que cuenta con el aval explícito de la inmensa mayoría de representantes estudiantiles, y por lo tanto que beneficia enormemente a todos los alumnos, dado que ahorra tiempo y evita costes de estancia y desplazamiento. Que UNIR ha informado de las implicaciones que tiene el uso del sistema de evaluación online, tanto del sistema de reconocimiento facial, que finalmente se canceló, así como del uso de la doble cámara. Han respondido a todas las preguntas que se han planteado, han elaborado documentos con preguntas frecuentes, así como diversas jornadas explicativas del sistema de evaluación.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación a la parte reclamada/ALIAS, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue recogido en fecha 31 de enero de 2022, como consta en el acuse de recibo que obra en el expediente.

Con fecha 16 de febrero de 2022 se recibe en esta Agencia escrito de respuesta indicando, en síntesis, lo siguiente:

a) Afirman que ninguna de las dos cámaras utiliza técnicas de reconocimiento facial, aportan certificado de SMOWLTECH que también lo confirma.

b) Afirman que NO se instala ningún programa en el dispositivo del alumno para el uso de la segunda cámara.

c) Afirman que al no utilizarse técnicas de reconocimiento facial ya no es necesario obtener el consentimiento del alumno puesto que no aplica esta base de legitimación. La base de legitimación es el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos por la Ley Orgánica de Universidades. Que esta misma Agencia afirmaba, en su informe 0036/2020, que este tratamiento estaba amparado por el artículo 6.1.e) del RGPD.

d) Afirman que el software instalado en los equipos nunca accede a información personal del interesado, salvo que el propio alumno acceda a estos datos mostrándolos en pantalla mientras realiza la prueba, puesto que el software captura el escritorio. No obstante, indican que UNIR ha informado a los alumnos sobre esta circunstancia. Si el alumno, en el transcurso de la prueba, accede a una ventana donde aparezca información no compatible con la prueba que realiza, el software realiza capturas de pantallas que

posteriormente son evaluadas por personal de la UNIR, y en el caso de que no acredite que el alumno ha realizado prácticas fraudulentas, se eliminarán.

e) Las garantías aplicadas para proteger los derechos y libertades de los interesados son:
   a. Realización de juicio de proporcionalidad.
   b. Garantizar un nivel adecuado de seguridad por parte del encargado de tratamiento SMOWL.
   c. Garantizar la privacidad por defecto y desde el diseño.
   d. Realización de los correspondientes análisis de riesgos y evaluaciones de impacto.
   e. Garantizar el principio de información en materia de protección de datos.

f) Indican que la evaluación de impacto y el análisis de riesgos ya fueron aportados en contestación a la reclamación del expediente E/05454/2021 y E/08977/2021.

g) UNIR considera que el sistema de evaluación online implementado no afecta de forma distinta al tratamiento de datos de carácter personal, con independencia de que el sistema cuente con un dispositivo adicional. En concreto, las exigencias sobre el uso de la doble cámara implican:
   a. El dispositivo tenga conexión a Internet y disponer de batería suficiente.
   b. Debe de enfocar al entorno, siendo visible:
      i. Las dos manos y cuerpo del interesado. No tiene por qué captar el rostro del interesado.
      ii. La pantalla de trabajo.

Con respecto a la afirmación aportada en el apartado f) anterior, tras analizar los documentos relativos al análisis de riesgos y la evaluación de impacto, se comprueba que no está incluido el uso de la segunda cámara utilizada por el dispositivo del alumno.

TERCERO: Con fecha 24 de febrero de 2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

Los antecedentes que constan en los sistemas de información son los siguientes:

1. En relación con el expediente E/05454/2021, tuvieron lugar las siguientes actuaciones:

    a. Tras varias reclamaciones presentadas en la AEPD sobre el uso de técnicas biométricas y de reconocimiento facial por parte UNIR, como responsable de tratamiento de datos personales, en fecha 14 de mayo de 2021 se da traslado a este responsable que contesta diciendo que la medida utilizada era ponderada, no solo no causando perjuicio sobre la protección de datos de carácter personal sino acreditando que las pruebas de evaluación se realizaban en condiciones óptimas. Justificaban que no existía medidas alternativas que garantizaran el resultado perseguido con igual eficacia. Indicaban también que se había realizado evaluación de impacto, concluyendo este con un riesgo bajo sobre los tratamientos llevados a cabo. Afirmaban que la medida no era desproporcionada, sino idónea, para alcanzar la finalidad perseguida. Todo ello sin perjuicio de que, si la AEPD consideraba que se había errado en el análisis, se cesara de inmediato en el uso del sistema objeto de valoración. En la respuesta de este traslado UNIR adjuntaba:
        i. El juicio de proporcionalidad
        ii. El contrato con encargado de tratamiento (SMOWLTECH)
        iii. La Evaluación de Impacto
        iv. Las Medidas de seguridad del encargado de tratamiento.
    b. No obstante, en fecha 14 de junio de 2021 se recibe un nuevo escrito por parte de UNIR aportando certificación de desactivación de reconocimiento facial para la monitorización de estudiantes.
    c. En fecha 27 de julio de 2021, la directora de la Agencia Española de Protección de Datos dicta resolución con una advertencia a la entidad reclamada para que adopte las medidas correctivas encaminadas a evitar que el tratamiento previsto pueda suponer un posible incumplimiento de la ley de protección de datos.

2. En relación con el expediente E/08977/2021, que tiene como origen una reclamación presentada en esta Agencia, se da traslado a la UNIR que posteriormente contesta aportando la siguiente información:
    a. Afirman que UNIR NO lleva a cabo un sistema de evaluación online basado en el uso de técnicas de reconocimiento facial, habiendo sido este eliminado y sustituido por un sistema de reconocimiento manual. Se aporta como anexo un documento entregado a ANECA donde se describe el sistema de evaluación llevado a cabo por UNIR, que está basado en el software SMOWLTECH y siguiendo el siguiente patrón de funcionamiento:
        i. Proceso de registro del alumno, se toman imágenes de la cara del alumno y DNI.
        ii. Durante el examen se aplica inteligencia artificial para la detección de objetos, pero nunca datos personales. Estas imágenes son almacenadas para su cotejo manual posterior.
        iii. Ante las alertas emitidas por el sistema de inteligencia artificial, se realiza revisión manual de las imágenes.

3. En relación con este expediente hay que destacar también el informe 0036/2020 de esta Agencia sobre cuestiones relativas al uso de técnicas de reconocimiento facial en la realización de pruebas de evaluación online.

QUINTO: Posteriormente a la recepción de este escrito por parte de UNIR, se recibe en esta Agencia nuevas reclamaciones que aportaban nuevos datos a esta investigación, decidiéndose entonces realizar un nuevo requerimiento de información al responsable de tratamiento UNIR, en fecha 27 de abril de 2022, en consonancia con la siguiente línea de investigación:

a) Conocer el análisis de riesgos actualizado incluyendo el uso de la segunda cámara, así como también la actualización pertinente de la evaluación de impacto.

b) Conocer más detalles sobre el software que se activa al escanear el código QR de la segunda cámara en el dispositivo del alumnado.

c) Aclaración sobre las condiciones que el alumno debe de aceptar en el momento de registro del software SMOWLTECH, previamente a la realización de los exámenes. Ya que, según prueba el contenido aportado en una de las reclamaciones recibida, entre las condiciones que el alumno debía aceptar se indicaba que la legitimación estaba basada en el consentimiento del usuario y que se realizaban modelos biométricos para comprobaciones de identidad, todo ello se acreditaba con capturas de pantalla adjuntadas en la reclamación recibida.

En fecha 17 de mayo de 2022 se recibe respuesta al requerimiento anterior por parte de UNIR, de su análisis se extrae:

a) Aportan el análisis de riesgos actualizado con el uso de la segunda cámara, concluyendo el mismo con un riesgo catalogado como ACEPTABLE, siguiendo para ello las herramientas de la AEPD (Evalúa-Riesgo RGPD y Gestiona EIPD). De este análisis de riesgos se extrae para la presente investigación:
   i. No se realizan tratamientos de categorías especiales de datos.
   ii. No aplican técnica de reconocimiento facial.
   iii. No utilizan tecnologías inmaduras o de reciente creación.
   iv. No resulta de aplicación el consentimiento, la base que legitima el tratamiento es interés público emanado del artículo 6.1.e) del RGPD, habilitado por el artículo 46.3 de la LOU.
   v. Se ha llevado a cabo el correspondiente juicio de ponderación y proporcionalidad.
   vi. Afirman que se informa debidamente a los interesados en el momento de la matrícula, así como en el Manual del Alumno. A su vez, si en las imágenes pareciera un tercero ajeno, se procedería a su eliminación o, en el caso que afecte a las calificaciones, se levantará acta de lo sucedido y se eliminarán.
   vii. Afirman que todas las evidencias recabadas por el software están sujetas a la revisión personal por parte de personal cualificado. Los empleados firman el correspondiente Manual de Funciones y

Obligaciones, así como reciben formación específica en materia de protección de datos para evitar violaciones de la confidencialidad.

viii. Se ha procedido a la correcta formalización del contrato de encargo de tratamiento, contándose con un protocolo para la selección y contratación de encargados de tratamiento.

b) El riesgo resultante de la evaluación de impacto, actualizada incluyendo el uso de la segunda cámara, es BAJO. De la misma se extrae como datos relevantes para esta investigación:
   i. Para garantizar la privacidad por defecto y desde el diseño, así como el principio de responsabilidad activa, afirman que el tratamiento estará sujeto a un proceso de revisión continua y a un sistema de mejora constante, realizándose para ello revisiones ordinarias (cada año académico de cara a las convocatorias ordinarias), y revisiones extraordinarias en caso de variación sustancial en el tratamiento de datos personales, como cambios en la tecnología aplicada, nuevas finalidades, nuevos datos…etc.

c) En relación con el funcionamiento del código QR en el dispositivo del alumno, indican que al escanearse el mismo se remite a una URL de SMOWL que solicita el permiso para acceder a la cámara, sin que comporte la instalación de ningún programa o software en el dispositivo del alumno. La captación de imágenes de esta segunda cámara se realiza desde la web. El flujo de información es el siguiente:
   i. Se escanea QR y se accede a la cámara desde la propia URL.
   ii. Se monitoriza la actividad del alumno a través del envío de imágenes periódicas.
   iii. En Smowltech se analizan (de forma automática) las imágenes recibidas para detectar posibles objetos fraudulentos en el entorno. En caso de detectarse posible fraude se eleva una alerta que debe ser revisada de forma manual por una persona cualificada.
   iv. No se toman decisiones automáticas y sin la intervención manual de una persona cualificada.

d) Envían, adjunto a la contestación del requerimiento, un video explicativo del uso de la segunda cámara con una completa descripción paso a paso de todo el proceso.

e) En relación con la información aportada en una de las reclamaciones, donde se adjuntaban varias capturas de pantalla del momento de registro de un alumno en la aplicación SMOWLTECH (requisito previo para la realización de los exámenes), y de las cuales se podía leer:
   i. Por un lado, en una de las pantallas mostradas se indicaba que la legitimación para el tratamiento de los datos personales estaba basada en el consentimiento del propio alumno.
      - Con respecto a este punto, UNIR contesta que esta información es errónea y no debería mostrarse en pantalla del alumno, y que, tras tener conocimiento de este hecho, "*desde UNIR nos pusimos en contacto con SMOWL y le requerimos la eliminación de este apartado, pues no es un reflejo fiel del*

proceso de evaluación de nuestros estudiantes, y adolece de incongruencias que no coinciden con la realidad". Adjuntan certificado de SMOWL donde garantizan que han procedido a solventar este error.

ii. Por otro lado, en otra de las capturas de pantallas aparecía un texto donde se le indicaba al alumno que se realizarían modelos biométricos para comprobaciones de identidad
   - Con respecto a este otro punto, UNIR contesta que tras tener conocimiento de esto se ha solicitado a SMOWL la comprobación y certificación de que, tal y como se indicó en su momento, no se procede al tratamiento de datos biométricos. Aportan nuevo certificado de SMOWL certificando que no se llevan a cabo tales tratamientos.

Con respecto al video aportado según el apartado d) anterior, tras su análisis queda constancia de que no hay instalación de aplicación software en el dispositivo del alumno.

Con respecto a las confirmaciones dadas por UNIR en el apartado e) anterior, y tras analizar los certificados aportados según los puntos i) y ii), se comprueba la veracidad y autenticidad del mismos, quedando constatado que:

1. Se corrige el error del software SMOWLTECH, eliminándose el apartado de la pantalla de registro donde se indicaba textualmente que "la legitimación para el tratamiento de los datos personales se basaba en el consentimiento del propio usuario".
2. Pese al mensaje que se mostraba en la pantalla por error, UNIR no realiza tratamientos de datos biométricos ni técnicas de reconocimiento facial.

Con respecto a lo anterior, hay que diferenciar entre la propia captura de imágenes del rostro del alumno para su almacenamiento y posterior revisión manual (por personal cualificado), y el uso de técnicas de reconocimiento facial, basadas estas últimas en el uso de software biométrico para mapear características de rostros y crear huellas faciales que posteriormente pudieran ser comparadas utilizando algoritmos específicos para verificar la identidad de una persona.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: "Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."

II

Tratamiento de categorías especiales de datos personales

El artículo 9 del RGPD, que regula el tratamiento de categorías especiales de datos personales, establece lo siguiente:

"1. Quedan prohibidos el tratamiento de datos personales 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 la orientación sexual de una persona física.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión o de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional;

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud."

III

Principios relativos al tratamiento

La letra a) y c) del artículo 5.1 del RGPD propugna:

"1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

(…)

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);"

El artículo 6 del RGPD, en su apartado 1, referido a la licitud del tratamiento establece lo siguiente:

"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones."

IV
Hechos denunciados

Las reclamaciones se concretan en que, durante los exámenes del mes de febrero de 2022, la UNIR estableció un sistema de identificación por medio de una herramienta informática, que han de instalar los alumnos, y utiliza algoritmos de reconocimiento facial. Ya que, en los exámenes indicados, la UNIR obligó a los alumnos a instalar una segunda cámara que enfocase el entorno del alumno. Entienden que el tratamiento realizado no es proporcionado y es altamente intrusivo puesto que puede grabar hasta a los familiares de los alumnos. Estiman, además, que el consentimiento no es libre ya que los alumnos con alto riesgo sanitario no pueden acudir a un examen presencial.

Sobre la utilización de técnicas de reconocimiento facial, tras verificar autenticidad del certificado aportado por la empresa SMOWL, queda constatado que no se realizan tratamientos de categorías especiales de datos y no aplican técnicas de reconocimiento facial.

Tras verificar la autenticidad de los certificados aportados por la empresa SMOWL, queda constatado que se ha eliminado la información que se aportaba (por error) en el proceso de registro del alumno en el sistema, en concreto la información errónea aportada sobre la base de legitimación y sobre el almacenamiento de modelos biométricos. La base de legitimación del tratamiento no es el consentimiento, sino que es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, la UNIR Quedando también constatado que UNIR no almacena modelos biométricos.

Asimismo, se ha verificado que no se instala software en el dispositivo del alumno, el acceso a la cámara del dispositivo se realiza desde una URL que solicita previamente permiso para acceder a ella. Esta segunda cámara tiene como única finalidad captar imágenes del entorno y enviarlas al encargado de tratamiento, y en caso de detectarse posible fraude se activa alerta que es revisada de forma manual por personal cualificado, por lo que nunca se toman decisiones automáticas en relación con las imágenes captadas por cualquiera de las dos cámaras.

Con respecto al software instalado en el ordenador del alumno, el principal objetivo de este es capturar el escritorio y hacer uso de la cámara frontal, por lo que no se accede a ninguna otra información personal almacenada en el propio dispositivo, salvo que el alumno la muestre en pantalla mientras se realiza la prueba.

De forma previa al tratamiento, la UNIR actualizó la Evaluación de Impacto para analizar e incluir los riesgos añadidos por el uso de la segunda cámara en los sistemas de evaluación, determinándose que el uso de una segunda cámara no supone un riesgo adicional que pueda afectar en mayor medida a los derechos y libertades de los afectados. En ella, se lleva a cabo el correspondiente juicio de ponderación y proporcionalidad con respecto a la inclusión de la segunda cámara, concluyéndose que la medida es necesaria y ponderada por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto, no existiendo otra medida más ponderada para la consecución del propósito con igual eficacia.

Se ofrece información completa al alumno en el momento de registro en la aplicación SMOWLTECH, y de forma previa a la realización de las pruebas, en concreto se transmite información adecuada sobre:

a. Responsable de tratamiento y delegado de protección de datos.
b. Finalidad del tratamiento y bases de legitimación aplicables.
c. Derechos de los interesados.
d. Plazos de conservación de la información, procedencia, destinatarios y sobre transferencias internacionales.
e. Sobre la seguridad de los datos.

V
Conclusión

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos.

Así pues, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a la UNIVERSIDAD INTERNACIONAL DE LA RIOJA con todos los anexos, y a cada reclamante, la resolución y el anexo correspondiente a sus datos.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

940-110422

Mar España Martí
Directora de la Agencia Española de Protección de Datos

ANEXO 0

A.A.A. (en adelante reclamante 1).

B.B.B. (en adelante reclamante 2).

C.C.C. (en adelante reclamante 3).

D.D.D. (en adelante reclamante 4).

E.E.E. (en adelante reclamante 5).

F.F.F. y D.D.D. (en adelante reclamantes 6).

B.B.B. *(en* adelante reclamante 7).

G.G.G. (en adelante reclamante 8).

H.H.H. (en adelante reclamante 9).

I.I.I. ***CARGO.1 (en adelante reclamante 10).

J.J.J. ***CARGO.2 (en adelante reclamante 11).

ANEXO I

A.A.A. (en adelante reclamante 1).

ANEXO II

B.B.B. (en adelante reclamante 2).

ANEXO III

C.C.C. (en adelante reclamante 3).

ANEXO IV

D.D.D. (en adelante reclamante 4).

ANEXO V

E.E.E. (en adelante reclamante 5).

ANEXO VI

F.F.F. y D.D.D. (en adelante reclamantes 6).

ANEXO VII

B.B.B. (en adelante reclamante 7).

ANEXO VIII

G.G.G. (en adelante reclamante 8).

ANEXO IX

H.H.H. (en adelante reclamante 9).

ANEXO X

I.I.I. ***CARGO.1 (en adelante reclamante 10).

ANEXO XI

J.J.J. ***CARGO.2 (en adelante reclamante 11).