- **Expediente N.º: EXP202100603**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: ***A.A.A.*** ciudadana británica con residencia en España (en adelante, la reclamante) con fecha 21/06/2021, interpuso reclamación en inglés, ante la Agencia Española de Protección de Datos. La reclamación se dirige contra **GSMA LTD.** con NIF ***N4004237F*** (en adelante, la reclamada). Los motivos en que basa la reclamación son los siguientes:

Fue invitada como ponente en la edición del MOBILE WORLD CONGRESS, (MWC) de junio 2021, celebrado en Barcelona. Con tal fin, se daba la opción de registrarse para el evento en "*virtual*", o "*presencialmente*". Para la opción en "*presencial*", "*la reclamada solicita cargar datos de categoría especial-detalles del pasaporte, incluyendo fotografías que se transfieren a un encargado situado en un país tercero-, para el reconocimiento facial con fines de seguridad*".

Manifiesta que la política de privacidad (https://www.mwcbarcelona.com/legal/privacy-policy), "e*stablece que la base del tratamiento es el consentimiento, sin embargo, en correo electrónico se ha declarado que se basa en el artículo 6.1 c), del RGPD, es decir, el cumplimiento de una obligación legal, haciendo referencia al artículo 22.2 de la LOPD y al artículo 11.1.h de la Ley Orgánica 2/1986. No es posible registrarse como ponente presencial sin cargar (subir) datos biométricos. A pesar de intentar solucionar la cuestión para encontrar una alternativa, ha sido necesario cargar mi pasaporte para el registro*."
Considera que no existe obligación legal valida para ese tipo de tratamiento de reconocimiento facial.

Por otro lado, ni las políticas de privacidad, ni las comunicaciones mantenidas con la reclamada a través del correo electrónico, proporcionan información clara sobre las transferencias de datos a un encargado del tratamiento en un tercer país.

Mientras en las políticas no se hace referencia a ningún subencargado del tratamiento, ni se reconocen transferencias a terceros, si se hace en documentos referenciados a través de las política de privacidad en un apartado de FAQ, https://www.mwcbarcelona.com/attend/event-entry/breez/breez-faq, en el que se indica que:

"*Si usted decide participar en BREEZ (siglas de Biometric Recognition Easy Entry Zone, zona de acceso fácil con Reconocimiento biométrico), sus datos biométricos serán comunicados al siguiente proveedor tercero que lleva a cabo las actividades de re-*

conocimiento facial del Evento: ScanVis Ltd.", considerando la reclamante que se está produciendo una transferencia.

En las comunicaciones con GSMA, han declarado en un correo electrónico: "*En relación con su cuarto punto, los servidores que procesan datos relacionados con ID se ubican en Europa. No hay transferencia de datos personales a Rusia. Nuestro proveedor de servicios elegido tiene una presencia global, a pesar de estar con sede en Bielorrusia. Tenga la seguridad de que la GSMA solo contrata a las empresas para que actúen en su nombre si dichas empresas son capaces de proporcionar representaciones y garantías contra la transferencia no autorizada a terceros*."

"*Aunque hemos solicitado a GSMA cualquier cláusula contractual estándar o reglas corporativas vinculantes pertinentes, no se ha proporcionado ninguna.*

"Con referencia a las recomendaciones del Comité Europeo de Protección de Datos (CEPD) sobre medidas que complementan las herramientas de transferencia para garantizar el cumplimiento del nivel de Protección de Datos personales de la UE, adoptadas el 10 de noviembre de 2020, creo que GSMA no ha considerado el riesgo potencial de transferencia a un tercer país a través del acceso remoto. Por lo tanto, la supuesta confianza en la adecuación como instrumento de transferencia legal no es eficaz."

Aporta copia de cadena de correos electrónicos intercambiados desde 20/05 a 4/06/2021, que se resumen:

- Reclamada, 20/05/2021, 10 h 16. Le asocia una "*invitación para el registro*". Le informa que ahora MWC 21 es sin contacto, para un mas rápido y seguro acceso, con verificación obligatoria de la identidad antes de la llegada para todos los asistentes. Para entrar al MWC 21 y a otros eventos asociados con la invitación. Asociado figuran los términos y condiciones indicando que la admisión está sujeta a ellos. Figuran links para: "*Como registrarse*". Una vez haya rellenado el "*registration system*" completo, "*recibirá una confirmación de email con mas información*". "*Por favor, tenga en cuenta: No hay áreas de apoyo al registro en la sede del MWC 21, así que asegúrese de que está totalmente registrado antes de su llegada a la sede. Algún error en ello podrá retrasar su acceso al evento"*.

- Reclamante**,** 20/05/2021, 10 h 39. "*me gustaría trasladarle mi preocupación sobre su solicitud obligatoria, que era opcional el año pasado, sobre subir/descargar mi documentación en su web*" "*El pasaporte o la tarjeta de identidad es una información muy privada y compartirla con un tercero que no es parte de una estructura gubernamental, ni es algo a lo que yo esté obligada por ley*" "*no proporciona información sobre como esta información se almacenará, se compartirá*".

- Reclamada, 20/05/2021**,** 11 h 41.Tenga en cuenta que este año se le requiere para "*subir*" su identificación. Hacemos esta verificación de identidad en el sistema de registro, ya que no se va a proporcionar credenciales impresas ni inscripción "*in situ*" (en el lugar).

"Usando tecnología de reconocimiento facial los asistentes pueden disponer de una verificación de la identidad instantánea cuando se registren utilizando la opción

BREEZ. Tomaremos la imagen de su pasaporte y usaremos tokens biométricos para emparejar esto contra la foto que haremos de usted durante el procedimiento de registro. Todas las personas que entren a España deben estar totalmente registradas para el MWC 21. Manifiesta que trabajan junto a los Mossos d´ Esquadra en el plan de seguridad para identificar y reconducir posibles amenazas de seguridad. *Recogiendo la identificación de los asistentes es uno de los medios para mejorar nuestra seguridad general y la de los asistentes*. Indica dos links de direcciones, uno de la *política de privacidad* y otro de los *términos y condiciones de asistencia* para ampliar esa información.

- Reclamante, 20/05/2021**,** a las 11:19 h, que insiste en que sus cuestiones no han sido contestadas.

- Reclamada, 28/05/2021, a las 10:46 h. Le indica que existe disponible información sobre el proceso que se requiere para la identificación, los destinatarios y el plazo de retención en una página de *registration faqs*, y en la de política de privacidad, así como en la del proceso de registro. "*En resumen, el GSMA organiza el MWC junto con las autoridades españolas. El pasaporte y los datos de identificación se requieren por la policía española, Mossos d' Esquadra. Tenga en cuenta que este no es un nuevo requisito. Sin embargo, la manera en la cual esta información se proporciona, electrónicamente, ha cambiado para 2021, debido a que los negocios necesitan tener un entorno sin contacto*"." *Dicho esto, tenga en cuenta que la identificación, los datos de identificación y el hecho de proporcionar el pasaporte, no es obligatorio para los titulares de pase virtual, que pueden asistir sin proporcionar tal información*."

- Reclamante, 28/05/2021, 11 h 26**.** Le indica que la web sugiere que la persona puede seleccionar, no optar (opt-out), por el registro automático, "*y es algo que me gustaría hacer*". También alude a que la web menciona las razones de salud para subir la documentación, pero ello no justificaría subir el pasaporte y la foto por no guardar relación, y que en la web se deduce que se transfieren los datos a una entidad bielorrusa, con los peligros que ello supone.

- Reclamada, 2/06/2021, 14 h, 53. Le explica que MWC 21 ofrece opciones, en persona y virtual. La virtual no requiere que suba un documento de identificación.
"*Si usted decide asistir en persona, entonces la verificación de la identidad es requerida por los Mossos d` Esquadra, policía española que no hace excepciones para los residentes en España. Todos los asistentes deben tener su identidad verificada*."

"*la medida no está relacionada con el COVID…*"" *En los anteriores Congresos todos los asistentes tuvieron que llevar su identificación en una tarjeta credencial. La novedad para este 2021 es que esa verificación será hecha digitalmente antes del evento, debido al entorno sin contacto. Para la verificación de la identidad en digital, a todos los usuarios se les requiere que suban una imagen de su documento de identidad y proporcionen una fotografía de ellos mismos. Los asistentes tienen dos opciones*:

-" *una verificación automática que usa tecnología de reconocimiento facial para emparejar la imagen del documento de identidad con su foto. Estos asistentes pueden usar las colas propias para el reconocimiento facial para acceder al evento".*

-Una verificación manual que se lleva a cabo por un agente que visualmente compara

las dos imágenes. Estos asistentes pueden acceder a la sede escaneando su código QR en su credencial digital la cual contiene su foto. Este proceso no usa ninguna tecnología de reconocimiento facial".

"*usted debe seleccionar la segunda opción si no desea la verificación automática".*

"En relación con su cuarto punto, los servidores que tratan los datos de identificación están establecidos en Europa. No hay ninguna transferencia de datos personales a Rusia. Nuestros proveedores de servicios seleccionados tienen una presencia global a pesar de que su sede central sea Bielorrusia. GSMA solo contrata a compañías que actúan en su representación si tales compañías son capaces de proporcionar garantías frente a transferencias a terceras partes."

- Reclamante**,** 2/06/2021, 16 h 18."*No quiero ser una conferenciante virtual. Pero no estoy segura de haber entendido como registrarme sin subir mi pasaporte. No me importa que se me verifique en el mostrador, pero no quiero que mis datos sean almacenados en ningún lado. Como procedo*? Añade que las autoridades locales pueden acceder a datos de compañías, a los servidores que operan en Bielorrusia.

- Reclamante, 3/06/2021 a las 11:10 h. "*Todavía no he recibido su respuesta sobre cómo proceder con el registro en el evento real sin descargar mis documentos"*

La fecha límite para el registro es el 6 de junio. Tenga en cuenta que las razones de seguridad mostradas en su web no es una base legal válida del artículo 6 del RGPD. Solicita, le envíe:

-Copia de las cláusulas contractuales estándar con la compañía en Bielorrusia
-La acreditación de que ha realizado una evaluación de impacto de las transferencias para determinar si las leyes de Bielorrusia son adecuadas.

-Especificar que medidas técnicas ha puesto en práctica para prevenir el acceso de las autoridades de Bielorrusia.

- Reclamada, 4/06/, 14 h y 59. Le indica que el tratamiento de sus datos tiene lugar en Europa y que utilizan cláusulas contractuales estándar, o decisión de adecuación de terceros países y otras herramientas legales para transmitir los datos fuera del Espacio Económico Europeo o Suiza. "*Mientras que el tratamiento del dato de identificación es relevante para conseguir objetivos de seguridad, requisitos establecidos por el articulo 22.2 LOPD y en el articulo 11.1h) para la aplicación de la Ley Orgánica 2/1986 , GSMA trata los datos como solicitan los Mossos d`Esquadra, en aplicación del artículo 6.1.c) del RGPD*."

- Reclamante, 4/06/2021, 17h 42**.** *"solicitando que explique que quiere decir ¿En cuanto cualquier dato personal del EEE y/o Suiza sean transferidos a un tercer país fuera del EEE o Suiza, excepto que sea un país con adecuación como lo define la Comisión, clausulas estándares u otra herramienta legal de transferencias sea ejecutada*."

Si *mi pasaporte no es un pasaporte de los países del Espacio Económico Europeo y Suiza, ¿significa esto que mis datos personales se transferirán fuera del EEE? Si este es el caso, me gustaría saber a qué país y ver las cláusulas contractuales tipo. Es un*

derecho del RGPD solicitarlo."

SEGUNDO: Por guardar relación y mencionarse bien en la reclamación, bien en los correos, se revisan;

a) Clausulado de "*términos y condiciones generales para la asistencia" MWC 2021, Barcelona*" en el que los asistentes tienen que aceptar dichas condiciones, figurando entre otras, la de registrarse en una cuenta en el sitio web, registrarse en el evento a través del sitio web, aceptar una invitación para un evento.
Consta: "*Identificación: Usted acepta llevar una identificación con foto emitida por su gobierno en forma de pasaporte o tarjeta de identificación nacional de la UE con usted en todo momento durante el Evento. Se le pedirá que presente dicha identificación. Usted es el único responsable de la exactitud de todos los datos personales proporcionados al registrarse para el Evento*…"

b) "política de privacidad", última actualización 29/04/2021.

En: "*Cuándo se aplica la política de privacid*ad", se aplica a diversos colectivos participantes en el MWC, entre otros conferenciantes o ponentes, asistentes, en relación con los datos personales obtenidos, vía: el sistema de registro de asistentes, la app del evento, tarjetas credenciales digitales y/o impresas, o el sistema de escaneo de reconocimiento facial (en los puntos de acceso, para sesiones o para participar en reuniones de espacios cerrados).

"Información que usted proporciona voluntariamente".

"Creación de cuenta y registro ": indica diversos modos de recoger datos con ejemplos "*cuando… creas una cuenta con nosotros, te registras para el evento, ...requieres un servicio…""La información recogida incluye, pero no se limita a: tu nombre, cargo, nombre de la empresa, dirección trabajo, email de trabajo, funciones laborales, número de teléfono, área de interés y fotografía. Si eres un ponente, como información adicional, tu perfil profesional*

"*Validación automática de identidad (reconocimiento facial, RF*)". Con su consentimiento, si elige registrarse en MWC Barcelona a través de "*validación de identidad automática"*, podemos tratar sus datos biométricos (mediante el uso de tecnología de RF) durante el proceso de registro en línea y cuando asiste al evento, estrictamente con los fines limitados de verificar su identidad. Si utiliza este proceso durante el registro, la tecnología de RF hace coincidir automáticamente la imagen que nos proporciona con la fotografía en su pasaporte/tarjeta nacional de identidad de la UE. Esta tecnología de RF analiza sus rasgos faciales tomando medidas de los puntos de datos que componen la cara. Estos puntos de datos incluyen la distancia entre sus ojos y la distancia desde frente a la barbilla, etc. La tecnología procesa una serie de puntos de datos para crear un *mapa de su cara en tiempo real*. Esto se convierte en un patrón de datos seguro utilizando un algoritmo complejo para crear su *token biométrico* (ficha biométrica, identificador).*Para fines de seguridad en el acceso al recinto, automáticamente haremos coincidir la imagen tomada en el punto de acceso contra su ficha token biométrica (es decir, su mapa facial*). Como se explica en el apartado: "*sus elecciones y selección de control*", debajo, puede

retirar su consentimiento para el uso de sus datos biométricos en cualquier momento. Si lo hace, eliminaremos su token biométrico y se llevará a cabo la validación manual_de la identidad, según sea necesario (aunque la retirada del consentimiento no afectará a la licitud del tratamiento de sus datos biométricos que ya haya tenido lugar en la etapa de registro). Haga clic aquí para obtener más información sobre cómo usamos las tecnologías de reconocimiento facial para fines de verificación de identidad.

Tecleando en dicho espacio, lleva a "*BREEZ FAQS -FR(Zona de fácil entrada con reconocimiento biométrico--Preguntas más frecuentes*". "*La forma conveniente de registrarse en MWC""* se basa en la tecnología de RF para proporcionar una identificación vía emparejamiento de foto en el registro en el sistema de registros online e identificar y verificar a los asistentes de las listas. Se presenta como "*tecnología de RF para* "*Proporcionar una verificación de identidad instantánea a través de la coincidencia de foto en el sistema de registro en línea, e Identificar y verificar a los asistentes inscritos para permitir el acceso a las instalaciones del evento y las áreas restringidas* (acceso al lugar BREEZ).
Los carriles libres están actualmente disponibles en los puntos de acceso perimetral del evento y en el perímetro del programa ministerial."

¿Quién puede usar BREEZ?
Todos los asistentes pueden usar BREEZ para acelerar su control de identidad en el sistema de registro de identificación automática de la identidad, además de aprovechar una funcionalidad de control de acceso más rápida y fluida durante los días del evento a través de BREEZ Venue acces. La inscripción en BREEZ es completamente voluntaria."

¿Cómo puedo inscribirme para usar BREEZ?
"Se puede inscribir en BREEZ durante el proceso de registro del evento o en cualquier momento después de haberse registrado para el evento *Siga estos sencillos pasos:*

1 "*Otorgar su consentimiento explícito para usar BREEZ*
2 "*Al dar su consentimiento se le indicará que le tomen una foto a través del sistema de reconocimiento facial ScanVis para la creación de su perfil biométrico*".
3 "*La fotografía cargada pasará por una verificación de calidad para garantizar que sea adecuada para el reconocimiento facial. Si se cumplen los parámetros definidos, se creará su perfil biométrico. Si no es así, se le pedirá que complete el paso anterior nuevamente."*
4. "*A continuación, se comparará su foto BREEZ con la foto de su pasaporte documento nacional de identidad de la Unión Europea utilizando su perfil biométrico y se producirá una puntuación de coincidencia. Si la puntuación está por encima del umbral del sistema, se confirmará su identidad, sino, sus fotos serán revisadas y comparadas por un ser humano. Esta es la validación automática de ID*".
5. *Una vez que se haya completado su registro (pago / código provisto), se le inscribirá en BREEZ y se beneficiará del acceso al lugar BREEZ*, *utilizando los carriles BREEZ en el lugar, para una experiencia sin contacto.*
Se acompaña un dibujo resumen con iconos titulado "*validación automática de identidad, qué es la validación automática de identidad* "*usaremos tecnología de*

RF para emparejar automáticamente la imagen que capturamos contra la fotografía en su pasaporte tarjeta nacional de identidad. Para hacer eso crearemos un token biométrico el cual contendrá la información sensible de los datos sobre sus características faciales únicas".

Viene en una serie de dibujos, en el primero "*no espera*": *"La validación de la identidad será completamente instantánea*. *La retirada de su consentimiento para usar sus datos biométricos para el acceso a la instalación, no afectará al tratamiento de datos biométricos que ya se hubiera efectuado para finalidades de validación de la identidad*".

En el segundo dibujo pone "*seguro y protegido*": "*Cuidamos de sus datos asegurándonos que se mantienen seguros. Para más información sobre cómo GSMA tratará sus datos biométricos, a quien pueden ser revelados y cómo retirar su consentimiento para el uso de estos datos biométricos para el MWC, por favor vea nuestro aviso de privacidad*."

Finalmente, el último dibujo: "*fácil acceso*": "*Para accesos a la instalaciones, el uso sin contacto de BREEZ en las colas verificará su imagen capturada por las cámaras contra su token biométrico para finalidades de validación de identificación.* "

También se indica en la parte inferior que "*Usted consiente para GSMA usando sus datos biométricos obtenidos de las fotografías proporcionadas por usted para finalidades de validación de identificación en el contexto del registro online y para el MWC Barcelona con finalidades de acceso a la sede",* precedido por una casilla que indica *"Si, consiento el uso de mis datos biométricos para la validación automática de identidad*".

¿Cómo puedo optar por no participar en BREEZ?"

Su consentimiento para participar en BREEZ sigue siendo válido mientras mantenga su cuenta del MWC o hasta que deje de participar en BREEZ.
Puede darse de baja de BREEZ retirando su consentimiento en cualquier momento accediendo a su cuenta de registro a través de https://register.mwcbarcelona.com/login y haciendo clic en el botón Cancelar inscripción en BREEZ, o contactando con registration@mwcbarcelona.com.

Si no da su consentimiento para el uso de BREEZ durante el proceso de registro, tiene la opción alternativa de validación común/estándar de ID manual (gestionada a través de nuestro Centro de contacto) en el momento del registro y el uso de una credencial digital (disponible en la aplicación de eventos My MWC app) para acceder al recinto. Su capacidad para asistir al Evento no se ve afectada por una negativa/retirada del consentimiento.

Si retira su consentimiento antes o durante el Evento, deberá usar su Credencial digital (disponible en la aplicación del evento My MWC) y escanearla cada vez que ingrese al Evento. Como se discutió anteriormente, además de proporcionar BREEZ Venue Access, BREEZ proporciona Validación de identificación automática durante el proceso de registro comparando la imagen de su pasaporte /

identificación nacional de la UE con su perfil BREEZ para verificar que el documento ingresado coincida con el registrante individual. Tenga en cuenta que la Validación automática de ID utiliza datos biométricos y ocurre instantáneamente durante el proceso de registro de BREEZ. El token biométrico creado para el proceso de comparación de imágenes se eliminará cuatro (4) semanas después de la finalización del Evento. Por lo tanto, si bien puede retirar su consentimiento de BREEZ en cualquier momento, no hay oportunidad de retirar el consentimiento de la Validación automática de ID una vez que se completa ese paso del proceso de registro.

Tenga en cuenta que aunque su consentimiento sigue siendo válido mientras mantenga su cuenta del MWC, sus datos biométricos solo se conservan durante 4 semanas después del Evento. Este es un paso importante para proteger su información. Solo cuando se registre en un Evento posterior con su cuenta del MWC, se volverá a generar el token biométrico.

¿Cómo se utilizan y almacenan mis datos biométricos?

"*Después de dar su consentimiento para BREEZ y cargar una foto, nuestro software de reconocimiento facial analiza las características faciales tomando medidas de los puntos de datos que componen la cara. Estos puntos de datos incluyen la distancia entre sus ojos y la distancia desde la frente hasta el mentón, etc. La tecnología procesa una serie de puntos de datos para crear un mapa en tiempo real de su cara. Esto se convierte en un patrón de datos seguro utilizando un algoritmo complejo para crear su token biométrico.*
Su "token biométrico" se almacenará y retendrá en la Unión Europea durante la duración del Evento y se destruirá de forma segura dentro de las 4 semanas posteriores al Evento. GSMA se compromete a proteger sus datos personales. Hemos implementado medidas técnicas y organizativas apropiadas para garantizar que sus datos estén seguros en todo momento. Cada token biométrico se cifra y almacena en una base de datos separada de los datos sin procesar utilizados en su creación.

Durante el proceso de registro, BREEZ se utiliza para comparar la imagen de su pasaporte/documento nacional de identidad de la UE con su perfil BREEZ para completar la Validación automática de identidad. En el Evento, BREEZ se utilizará con el fin de identificar a los asistentes inscritos para proporcionar acceso a BREEZ Venue. Cuando ingrese al carril BREEZ y se acerque a una cámara, será reconocido y se le otorgará acceso al Evento. Esto se realiza haciendo coincidir la imagen en tiempo real de su rostro con el token biométrico creado durante el proceso de registro."

¿A quién se divulgan mis datos biométricos?
"*Si elige participar en BREEZ, sus datos biométricos se divulgarán al siguiente proveedor externo que lleva a cabo las actividades de reconocimiento facial para el Evento: ScanVis Ltd*."

Si BREEZ no tiene contacto, ¿puedo dejar mi credencial digital y mi identificación en el hotel?"

Todos los asistentes deben tener su credencial digital disponible para ingresar al perímetro externo del lugar. La credencial digital también será la única forma de acceder a conferencias o sesiones de socios.
Todos en España están legalmente obligados a llevar una identificación o pasaporte válido en todo momento. Por lo tanto, los asistentes deben conservar dichos documentos de identificación con ellos durante el Evento."

CONTINUA EL APARTADO DE POLITICA DE PRIVACIDAD:

Escaneo de tarjetas/credencial
"Nosotros, o los terceros autorizados que participan en el Evento (incluidos los expositores y patrocinadores), podemos recopilar sus datos personales escaneando su credencial digital. Esto puede ocurrir cuando accede o sale del lugar, ingresa a sesiones u otras áreas restringidas en el Evento, o ingresa a un espacio cerrado, sala de reuniones o restaurante. Este escaneo puede ocurrir con fines de control de acceso, análisis, planificación de eventos, logística, salud y seguridad (incluida la prevención de la propagación de enfermedades y fines de seguimiento de contratos) y para compartir con un proveedor de sesión externo si ha escaneado su credencial digital o registrado para asistir a la sesión de ese tercero.

"*Compartir información* ",
"no vendemos información personal a nadie y tampoco revelamos tus datos personales a terceras partes para uso independiente, a menos que": (se destacan solo algunos puntos)

"Has consentido que tu datos biométricos obtenidos a través de tecnología de reconocimiento facial durante los registros para el acceso y a la sede sean accesibles por terceras partes-haz clic aquí para mas información de quienes son estas terceras partes".

"Se proporciona a cualquier organismo competente encargado de hacer cumplir la ley , regulador, agencia gubernamental, tribunal u otro tercero, hacer cumplir un acuerdo que tenemos con usted o para proteger nuestros derechos, propiedad o seguridad, o los derechos, propiedad o seguridad de nuestros empleados u otros. Esto incluye los organismos encargados de hacer cumplir la Ley correspondiente con fines de seguridad y las autoridades sanitarias, según sea necesario para prevenir la propagación de enfermedades, incluido el Covid-19(por ejemplo, con fines de rastreo de contactos o para facilitar la entrada en España).

"*Base legal para el tratamiento de información personal"*

"…*normalmente recopilaremos su información personal solo cuando tengamos su consentimiento para hacerlo, cuando necesitemos la información personal para realizar un contrato con usted, o cuando el tratamiento sea nuestro interés legítimo y no sea anulado por sus intereses de Protección de Datos o derechos y libertades fundamentales. En algunos casos, también podemos tener la obligación legal de recopilar su información personal cómo es posible que se nos solicite hacerlo por razones de interés público o que necesitemos la información personal para proteger sus intereses vitales o los de otra persona, por ejemplo en caso de una emergencia médica durante el evento. Si le solicitamos que proporcione información personal para cumplir con un requisito legal o para realizar un contrato con usted, lo dejaremos claro y le informaremos si la*

provisión de su información personal es obligatoria o no (así como las posibles consecuencias si usted no proporciona su información personal. Estamos legalmente obligados a proporcionar los datos personales de los asistentes y el personal del proveedor, es decir nombre, fecha de nacimiento, nacionalidad, tipo número de documento y fecha de emisión, a las autoridades encargadas de hacer cumplir la ley en relación con la seguridad del evento. Cualquier fallo en proporcionar esta información significará que no podemos sin registrarlo para el evento y/o permitirle acceder al lugar."

"Transferencia de su información al Espacio Económico Europea EEE, Reino Unido y Suiza."

Informa que GSMA Ltd tiene su sede en EEUU. "*Al usar su información como se establece en esta política de privacidad, puede transferirse a países fuera del EEE, el Reino Unido y Suiza. A modo de ejemplo, esto también puede suceder si una de nuestras empresas asociadas o nuestros proveedores de servicios se encuentran en un país fuera del EEE, el Reino Unido o Suiza. Cuando transferimos datos personales desde el EEE, el Reino Unido y Suiza a otros países, utilizamos una variedad de mecanismos legales, incluidas las clausulas contractuales estándar adoptadas por la Comisión de la UE para garantizar que sus derechos y protecciones viajen con sus datos.*

"Retención de datos"
[…]"

"*Cuando haya dado su consentimiento para la validación automática de identidad, eliminaremos su token biométrico (su mapa facial) dentro de los 28 días posteriores al último día del evento*".

"Tus elecciones y control"
[…]"

"*Del mismo modo, si hemos recopilado y tratado su información personal sobre la base de su consentimiento, puede retirarlo en cualquier momento*"

"*Cuando tratamos sus datos personales automáticamente, por ejemplo cuando llevamos a cabo la validación automática de identidad, tiene derecho a impugnar una decisión de denegarle la entrada al evento basándose únicamente en esta validación automática de identidad en la medida en que dicha decisión tenga un fundamento jurídico o un efecto significativo similar en usted. En tales circunstancias, tiene derecho a expresar su punto de vista y solicitar una revisión humana de la decisión . Puede ejercer este derecho comunicándose con el centro de contacto antes del evento, en cuyo caso puede ser necesario validar manualmente la identificación y/o realizar otros controles de seguridad apropiados*".

El apartado último, "*contáctanos*", indica: "*Si en cualquier momento quiere contactar con nosotros con sus opiniones sobre nuestras practicas de privacidad o cualquier otra consulta relativa a su información personal, o si no quiere que continuemos usando su información como se ha señalado arriba, puede solicitarlo por e mail a dataprivacy@gsma.com o escriba a Data Privacy-Legal, GSMA Ltd. The Walbrook Buiding 25 Walbrook, London."*

TERCERO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5/12, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación a la a la parte reclamada, -sede de Londres – E/8199/2021, 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, y en concreto:*

1. La decisión adoptada a propósito de esta reclamación.

2. Informe sobre las causas que han motivado la incidencia que ha originado la reclamación.

3. Informe, si procede, sobre las medidas adoptadas para adecuar su "Política de Privacidad" al artículo 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (RGPD), fechas de implantación y controles efectuados para comprobar su eficacia.

4. Justificación de la base jurídica en la que se apoya el tratamiento de datos biométricos, circunstancia que levanta la prohibición para tratar categorías especiales de datos, según el artículo 9 del RGPD, así como la necesidad de aportar una copia del documento identificativo para la acreditación de los asistentes al evento.

5. La finalidad del tratamiento.

6. La información facilitada a los interesados sobre el tratamiento de sus datos biométricos y, en su caso, para la obtención de su consentimiento.

7. Motivos que justifican la necesidad y la proporcionalidad del uso de los datos biométricos para la finalidad perseguida.

8. Medidas adoptadas para garantizar que no es posible la reutilización de los datos biométricos para otra finalidad.

9. Medidas de seguridad adoptadas para proteger la confidencialidad de los datos personales

10. La Evaluación de Impacto realizada o motivos por los que no se ha realizado (para conocer la lista de tratamientos de datos personales que requieren una evaluación de impacto, así como cualquier otra información relacionada con las evaluaciones de impacto, puede consultar la herramienta "Gestiona EIPD" en https://www.aepd.es/es/guias-y-herramientas/herramientas/gestiona-eipd)

11. Informe sobre si se realizan transferencias internacionales y, en su caso, si existe decisión de adecuación o garantías adecuadas en materia de transferencias internacionales de datos.

12. Documentación acreditativa sobre la relación entre el responsable y el encargado

de las actividades relacionadas con el reconocimiento facial.

13. Informe sobre las medidas adoptadas para evitar que se produzcan incidencias similares, fechas de implantación y controles efectuados para comprobar su eficacia.

14. Dirección postal de su representante en la Unión Europea.

15. Cualquier otra que considere relevante.

Con fecha 10/09/2021, se recibe en esta Agencia escrito de respuesta que lleva la indicación GSMA Ltd., en una dirección de Atlanta, USA. Comienza indicando: "*Le escribo en representación de GSMA Ltd. (GSMA) en relación con la carta enviada E/8199/21*…".

Según información de internet, GSMA (Global System for Mobile Communications, "*Sistema Global para Comunicaciones Móviles*), es una organización de la industria del móvil que agrupa a operadores de todo el mundo, mas de 750 operadores de telefonía móvil y mas de 400 Compañías están asociadas como miembros. En la web www.mwcbarcelona.com/legal que contiene información sobre el Congreso de Barcelona 2022, se indica que "*GSMA LTD con su principal lugar de negocio localizado en Atlanta, USA, subsidiaria de propiedad entera de la asociación GSM, y con respecto a 4yfn 2022, GSMA 4fyn EVENT MANAGEMENT S.L., una subsidiaria de GSMA LTD., le da la bienvenida al MWC BARCELONA 2022.",* y que "*GSMA LTD y sus afiliados le proporcionan el evento*…"

En la respuesta, indica:

1) La reclamante y la reclamada continuaron en contacto después de la última copia de correo de 4/06/2021 y se logró una resolución satisfactoria "*se registró para el Congreso como asistente virtual y tomó parte como orador en una mesa redonda*", y la reclamada le proporcionó un "*pase virtual gratis*" y no se le solicitó descargar o subir un documento de identidad que era el elemento sobre el que iba su reclamación. No resulta cierto pues que la reclamada "*subiera el pasaporte*".

2) Aporta, a efectos clarificadores las manifestaciones que se contienen en la reclamación y la corrección que estima la reclamada, debido posiblemente a "eventuales malentendidos."

a) Sobre que el evento en presencial o virtual, GSMA requiriese subir o cargar datos como el pasaporte, que se transfieren a un encargado en un tercer país, manifiesta que:

-Era preciso un control de identificación para toda la asistencia presencial a la conferencia. La validación de la identidad por FR (reconocimiento facial) era opcional. La comprobación de identidad no era necesaria para la mayoría de los pases virtuales.

"*Había una opción para que la validación de la identidad se llevara a cabo sin el uso de FR"* . "*La solución FR era solo una de las tres opciones para la validación de identidad puestas a disposición*". Las opciones incluyen:

- la validación de la identificación con FR,
- la validación manual de identificación enviada en línea, (standard ID validatión-validación común de identidad).

- y en circunstancias limitadas, la validación de identificación en papel ,presencial, in situ.

Considera por tanto que no es del todo cierto que: "*no es posible registrarse como orador presencial sin cargar datos biométricos*". Solo la opción de identificación con FR incluía el tratamiento de datos de categorías especiales, para los cuales se obtenía el consentimiento explicito.

b)Sobre la discordancia en la base legitimadora del tratamiento que deriva de la clausula de política de privacidad, manifiesta que no todas las formas de verificación de la identificación requerían el uso de tecnologías FR y que el consentimiento explícito es la base jurídica sobre la que se han tratado los datos de FR, no habiendo discrepancias en la información proporcionada por la reclamada, en cuanto a que se indica que la base del tratamiento en el correo electrónico que dice la reclamante haber recibido se indicaba el artículo 6.1 letra c) del RGPD, ya que, "*separadamente, se le exigió a GSMA por Ley que facilitara determinada información a los Mossos-nombre apellidos nacionalidad, fecha de nacimiento, documento de identidad facilitado, fecha de expedición y número de documento.*"

c) La información sobre transferencias de datos y encargados de tratamiento no se contiene en la política de privacidad. Se optó por proporcionar esa información a través de una página de preguntas frecuentes, FAQ, para que fuera fácilmente accesible, figurando así en https://mwcbarcelona.com/attend/event- entry/breez/breez-faq donde se contienen también los proveedores de servicios.

En cuanto a la manifestación de la reclamada de que "*esto establece que los opt-outs están disponibles, sin embargo, después de la correspondencia por correo electrónico, esto es incorrecto. Un opt-out solo está disponible para asistencia virtual*".

Manifiesta que en "*preguntas frecuentes*", se refieren al derecho a retirar el consentimiento en la sección "*Cómo puedo darme de baja de BREEZ*". "*El Interesado analiza esta opción en el contexto del registro (pero no se relaciona con las opciones disponibles en la etapa de registro). Además, para la finalidad de registro, es incorrecto decir que, excepto para asistencia "virtual", los solicitantes de registro se les exigía enviar para el RF una copia de la identificación. Se requería una copia de identificación en todos los casos excepto (la mayoría) de los pases de asistencia virtual, pero FR era opcional y se invitaba a los solicitantes de registro a consentir expresamente para el tratamiento de sus datos biométricos. Los solicitantes de registro podrían optar por una validación de identidad estándar en lugar de FR, que no perjudica su capacidad de registrarse para la conferencia. Del mismo modo, no recibimos quejas de que optar por una validación de identificación estándar en lugar de FR afectara adversamente la experiencia de la conferencia*." "*Al MWC 2021,*

asistieron aproximadamente 20.000 delegados y nuestro equipo de registro recibieron muy pocas consultas en relación con los procesos de verificación de identidad, la mayoría de los cuales eran de carácter técnico".

3) Manifiesta que su política de privacidad se actualizó para el MWC 2021, siendo su última versión, 29/04/2021.

4)"*Preguntas FR: Se utilizaron tecnologías FR (cuando la persona optó por esta opción y dio su consentimiento expreso) para verificar la identidad de los delegados en el evento, por fines de seguridad. Esto se dio en ambos supuestos:*

-Cuando la persona se registra online, esto es, FR es usada para comparar una foto de la persona tomada al tiempo del registro con la foto del documento de identidad que se sube por ellos, y ,

-Para permitir el acceso a las instalaciones del evento, (es decir, se verificó el token biométrico en el pase de los delegados) automáticamente contra su imagen utilizando tecnologías FR).

Como se explicó anteriormente, los delegados pudieron elegir la verificación de identificación común, que no implicó el uso de tecnologías FR. En cambio, las personas tenían la opción de cargar una copia de su documento de identidad y una foto (tomadas en el momento en que se registraron) que luego fueron revisadas manualmente por un tercero contratado por GSMA para estos propósitos. Su acceso fue facilitado por personal de seguridad revisando la imagen almacenada en su pase de conferencia frente a su aspecto/apariencia

En una pequeña cantidad de casos, verificaciones de identificación manuales en persona (es decir, verificando la versión en papel de los documentos de identificación) también tuvieron lugar en el lugar del evento (aunque de manera excepcional para minimizar la propagación de covid-19, como se detalla a continuación) y solo se realizó para ciertos tipos de pases.

La verificación de identidad no se realizó en relación con la mayoría de los delegados que asistieron al evento de manera virtual.

Como se describió anteriormente, solo se requería FR como una de las tres opciones disponibles para registrarse presencialmente para el evento.

Como también se indicó anteriormente, la GSMA compartió parte de la información obtenida en el contexto de la verificación de identidad (excluida la información biométrica cuando se recopile) con los Mossos, ya que legalmente se exige de conformidad con el artículo 11.1.h de la Ley Orgánica 2/1986, de Orden Público. Por motivos de seguridad, y con el fin de garantizar que capturó información confiable del documento de identidad, la GSMA exigió la provisión de una copia del documento de identidad.

En el MWC 2019, GSMA permitió que las copias en papel de los documentos de identificación se verificarán manualmente al acceder a la sede de MWC. Sin embargo esta opción se suprimió-salvo excepciones- por razones de salud y seguridad para el

evento de 2021, con el fin de minimizar el riesgo de propagación de la COVID-19, reduciendo colas y las multitudes en los puntos de acceso. Esto está en consonancia con el "plan de acción de congresos de la Generalitat de Cataluña" al que está sujeto a la GSMA y que exige expresamente la sustitución de procesos manuales por procesos digitales Aporta el link de este plan, de 22/07/2020. Contiene directrices y recomendaciones para la reducción del contagio por coronavirus para reuniones y congresos, que se aplica a los organizadores de conferencias, congresos o convenciones, responsables de la implantación y coordinación de medidas entre las que se incluyen la elaboración de un plan de contingencia para reducir los riesgos de la COVID 19.

En el punto 4.2.3.2 "*control de accesos registro e inscripciones",* se indica que para gestionar adecuadamente los flujos de entrada y salida y el tráfico de personas, se establecen las siguientes medidas generales: fomentar las gestiones y pagos en línea y la sustitución siempre que sea posible de los procesos manuales por otros digitales, envío de acreditaciones en línea, descarga de acreditaciones en el móvil, fomentando los medios sin contacto y gestionar las colas con cintas separadores.

Las tecnologías FR también se usan para mejorar la seguridad. El MWCB es un evento clasificado como "amenaza de alta seguridad" por las autoridades españolas. La verificación de la identificación con FR es eficaz para lograr el objetivo perseguido, es decir la seguridad en un entorno sin contacto.

Los delegados que habían elegido la validación de identificación común o estándar, utilizaban líneas de entrada separadas a las de las líneas de FR. Ellos escanearon su pase digital y el personal de seguridad compara la imagen almacenada en el pase digital que se mostró en una pantalla con la apariencia del delegado. Esto se hizo a cierta distancia dado el entorno sin contacto que la empresa consideraba poco probable que fuera tan preciso como el control de identificación realizado con tecnologías FR especialmente en el contexto de tratar de garantizar un flujo rápido de delegados para evitar el hacinamiento.

Los controles de identificación de acceso del FR también fueron más rápidos, lo que redujo el tiempo de espera y congestión dentro de un espacio cerrado."

Los datos biométricos retenidos se eliminaron al final del evento, solo unas pocas semanas después registro y unos días después de su tratamiento para fines de control de acceso. Estas medidas protegen los datos de ser utilizados para fines distintos a la validación de identidad.

La página que se incluye en "privacy policy" da información sobre el proceso de validación de la identificación automática, FR, lleva a información especifica sobre el BREEZ (capas) y esta página explica la posibilidad de elegir verificación de la identificación común, sin el uso de la tecnología FR".

Los delegados tienen una verdadera opción entre comprobar su identificación utilizando tecnologías FR o manualmente. La principal diferencia entre ambos es que la opción FR permite que el proceso de registro en línea se complete inmediatamente, mientras que la verificación manual de identificación requerirá una breve espera de unos pocos días para confirmar el registro. Este breve retraso no afectó a la capacidad

de las personas para registrarse para la experiencia en persona ni retrasa la participación en el evento.

Evaluación de impacto sobre protección de datos

No es aportado, bajo la justificación de que "*GSMA ha llevado a cabo una evaluación de impacto sobre la protección de datos en relación con el uso de tecnologías FR, y este documento se está revisando actualmente en preparación para nuestro evento MWC 2022*."

Transferencias internacionales de datos

GSMA tiene un contrato con un tercero proveedor de servicios (*ScanVis Limited*) , que no es aportado, para la prestación de servicios de FR. "*Nuestro compromiso contractual con ScanVis incluye el requisito de implementar medidas de seguridad adecuadas para proteger los datos personales tratados por el proveedor de servicios y se ajusta al artículo 28 del RGPD*."

SCAN VIS tiene sede en Hong Kong, sin embargo, los datos del MWC FR están alojados por Amazon Web Services («AWS») en Alemania. Como SCAN VIS se encuentra en un país no adecuado fuera de la UE, la GSMA ha suscrito cláusulas contractuales estándar con *SCAN VIS.*

Además, como salvaguardia adicional, los datos biométricos se encriptan y solo el algoritmo en sí puede entender lo que significa.

La GSMA no transfiere datos personales a Bielorrusia o Rusia, como cuestionó la interesada.

Nombramiento de un representante de la UE

"*GSMA EVENT PROJECT MANAGEMENT, S.L. (EPM) es una filial española de GSMA. EPM se ha creado específicamente para prestar servicios relacionados con la gestión del MWC en Barcelona. Las actividades de tratamiento de datos personales de la GSMA están inextricablemente vinculadas a las actividades de EPM.*

Por lo tanto, la GSMA trata datos personales en el contexto de las actividades de un establecimiento de la UE y está sujeto al RGPD con arreglo al artículo 3, apartado 1 del RGPD, de modo que no se requiere ningún representante de la UE de conformidad con el artículo 27 del RGPD."

No proporciona el NIF de esta entidad, dirección ni reseña identificativa alguna.

CUARTO: En el Registro Mercantil (RM), se realiza búsqueda bajo GSMA y solo figura registrada *la entidad GSMA 4YFN EVENT MANAGEMENT S.L, CIF* ***B67299297****, domicilio* Av. de la Reina Maria Cristina S/N Hall 1, Barcelona, objeto social "*prestación de servicios de conferencias y eventos. organización de eventos empresariales, sociales, culturales, recreativos o tecnológicos, incluyendo puesta en*

marcha de ferias de muestras, etc.". En la consulta a la aplicación AXESOR, figura como socio único GSMA LIMITED. A GSMA LIMITED le figura en la aplicación AXESOR como entidad no residente, el NIF ***N4004237F***.

En la web https://www.dnb.com/business-directory/company-profiles.gsma_ltd.9e65a-aadc5cdd92b48292ac68a42aff7.html, figura que GSMA LIMITED tiene 105 empleados y 37,12 millones de dólares de ingresos.

QUINTO: Con fecha 21/09/2021, por aplicación del artículo 65.5 de la LOPDGDD, prosigue la tramitación de la reclamación.

SEXTO: Con fecha 9/06/2022, la Directora de la AEPD acordó:

"INICIAR PROCEDIMIENTO SANCIONADOR a GSMA LTD., con NIF ***N4004237F****, por la presunta infracción del artículo 35 del RGPD, tipificada en el artículo 83.4.a) del RGPD y en el artículo 73.t) de la LOPDGDD*"

"*A los efectos previstos en el art. 64.2 b) de la ley 39/2015, de 1/10, del Procedimiento Administrativo Común de las Administraciones Públicas, la sanción que pudiera corresponder sería de multa de 200.000 euros, según lo especificado, sin perjuicio de lo que resulte de la instrucción*."

SÉPTIMO: Con fecha 27/06/2022, la reclamada indica:

1) En su escrito a la AEPD de fecha 10/09/2021, GSMA facilitó respuestas detalladas a las preguntas de la AEPD. GSMA no interpretó que la pregunta relativa a las evaluaciones de impacto relativas a la protección de datos ("*EIPD*") se refiriera a que la AEPD estaba solicitando la aportación de una copia de dicha EIPD, sino que pedía confirmación de que se había realizado una EIPD. Conforme a esta interpretación, GSMA confirmó que había llevado a cabo una EIPD para el uso de tecnologías de reconocimiento facial ("*RF*") y que se estaba actualizando el documento para el MWC22.

Reiteran que la reclamante no se registró en modo de uso de tecnología "*RF*", "*por ello, no consideramos que la EIPD de RF fuera relevante a efectos de esta reclamación en concreto y se interpretó de esa forma*".

2) Aportan copia de la EIPD de 12/01/2020 realizada usando el sistema "One Trust" "ya existente cuando se solicitó" y otra que la sustituye, actualizándola para el MWC22. "La reclamada no obvió la necesidad de mitigar los riesgos derivados del uso de las tecnologías de RF para el evento 2021", "las cuales tuvieron en cuenta la información y evaluación de la citada EIPD 2020" y "la necesidad de minimizar el riesgo de diseminación de la COVID-19", y tomó las siguientes medidas prácticas:

a) "*la opcionalidad del tratamiento de datos biométricos y las medidas para asegurar que la opción de verificación de identidad manual (sin el uso tecnologías de RF) no fuera en detrimento del usuario*;

b) "*la provisión de información relativa a los tratamientos de datos biométricos en capas y de un modo fácil para el usuario*;"

c) *"la implementación de medidas de seguridad físicas y técnicas robustas parar proteger los datos biométricos;"*

d) *"la imposición de medidas de seguridad robustas a ScanVis, el proveedor de tecnologías de RF, incluyendo evaluaciones de seguridad por parte de GSMA; y*

e) *"el borrado de la información biométrica en breve, tras la finalización del evento."*

2) El informe de evaluación de impacto, DATA PROTECTION IMPACT ASSESMENT (DPIA en inglés, EIPD en español), de 12/01/2020, tiene las siguientes características:

-creado el 17/12/2019, fecha de remisión 12/01/2020, nombre "*MWC 20 proceso de reconocimiento facia*l", en lengua inglesa.

-se divide cuestiones a valorar, respondiendo si o no, y una explicación en su caso. Tiene 9 partes. La primera: parte general desglosada en 9 preguntas, la segunda: identificación de las partes que forman parte del tratamiento y tiene 3 preguntas, la tercera: licitud y transparencia con 11 cuestiones, la cuarta: derechos de los interesados y exactitud, con 12 cuestiones, la quinta: limitación de la finalidad con cuatro cuestiones, la sexta: minimización de datos, con 5 cuestiones, la séptima: limitación del almacenamiento, con 5 preguntas, la octava: integridad y confidencialidad, con 11 cuestiones y la novena: información adicional. Los resultados que constan son 0 en toda clase de riesgos, riesgo residual, ninguno. Se ha de significar:

a) En el primer apartado: "*general*", se indica que "*es una nueva versión del proceso de reconocimiento facial actualizado para el 2020*" (en el se mencionan eventos fechados en el Congreso de 2020, ninguno de 2021), y que *BREEZ es el término orientado al cliente para nuestro proceso de reconocimiento facial*". Es una revisión del proyecto de 2019, en la que se incluyen sus cambios desde entonces, refiriendo:

-Desarrollo de un widget (dispositivo, aplicación) de inscripción completamente nuevo.

- El principal método promocionado de captura de fotos es a través de una *selfie* para garantizar que la foto capturada sea reciente. Los usuarios todavía pueden subir una foto si es necesario.

- La captura de *selfies* incluye orientación y comentarios en tiempo real para garantizar que la cara esté en la posición correcta y sea aceptado por el algoritmo FR. Hay mensajes de error específicos para guiar al usuario en caso de la foto *BREEZ* capturado/proporcionado siendo rechazado.

- El widget de inscripción también incluye una comprobación de verificación de FR en tiempo real para asegurarse de que la persona que se inscribe pueda ser reconocido por el sistema. El usuario puede omitir este paso si es necesario.

- Inscripción BREEZ promovida desde dentro del proceso de carga de foto de perfil.

- Integración de un nuevo widget que permite a los asistentes escanear su pasaporte/ID de la UE; esto extraerá los datos de la zona legible por máquina (MRZ), así como la fotografía en la identificación.

- La foto capturada del pasaporte/ID de la UE se compara con la foto capturada durante el registro de *BREEZ* para determinar la probabilidad.

- Inclusión del concepto de Secured Attendee Profile (SAP) lo que significa que a través del proceso de automatización el asistente, ha:

a) proporcionado los detalles de su pasaporte/ID de la UE
b) se ha inscrito en el programa *BREEZ* FR
c) la foto del Pasaporte/ID de la UE coincide con la foto proporcionada para BREEZ.

Señala que en la realización de la DPIA ha participado su "*equipo de Proteccion de datos*", junto a la mención del articulo 35.2 del RGPD que indica la participación del Data Protection Officer.

El propósito de este proceso es agilizar los procesos manuales en el sitio en el momento de la recogida de credenciales y brindar un servicio eficiente.(1*.7 finalidad de las operaciones de tratamiento propuestas.)*

b) En el apartado de licitud y transparencia, (3.1) se indica que el consentimiento que es la base de tratamiento, es solicitado de forma libre, informado, específico y sin ambigüedad, guardándose la acreditación del consentimiento. (3.3).
método para que los asistentes accedan a MWC/4YFN.

a) en la pregunta 4.3*, ¿cuándo los datos personales sean transferidos a un tercer país o a una organización internacional, tendrá el sujeto interesado el derecho a ser informado de las adecuadas salvaguardas proporcionadas por el responsable o el encargado? y se indica que sí.*

b) indica en la pregunta 4.4, que: "*todos los datos biométricos recogidos para las finalidades de este proyecto serán borrados como fecha fin el 26/03/2020*" (no obstante se está analizando el Congreso del año 2021). "*El resto de los datos en concordancia con los períodos de guardado de datos de 5 años se almacenarán , a menos que haya una solicitud para su borrado*."

c) En la pregunta 5.1 "*limitación de la finalidad*" de la respuesta que se da, se indica que*: "los asistentes para él Mobile World Congress tienen la oportunidad de apuntarse al programa de FR hasta el 27/02/2020*".

e) En la pregunta 5.2, ¿*cómo valoraría la necesidad de las operaciones de tratamiento propuestas?, la respuesta es media, y la justificación: "Con el fin de satisfacer las medidas de seguridad en el evento, hemos sido instruidos por el formulario de la*

Policía Española para poner en marcha procesos estrictos para garantizar que todos los asistentes sean examinados a través de una verificación de pasaporte/documento de identidad de la UE antes de que puedan

- recoger su distintivo-credencial
- cada vez que ingresen al recinto.
Los procesos anteriores se basan en verificaciones manuales que pueden ser lentas y brindar una experiencia negativa en el evento.
A través del uso de la tecnología descrita en este DPIA, podemos automatizarlos para permitir un uso mucho más
eficiente, así como un evento más preciso y seguro."

f) En la cuestión 5.3, se indica: *"¿si las operaciones de tratamiento propuestas son proporcionales a su finalidad?",* se incluye el artículo 35.7 B en su redacción, y la respuesta es sí, indicando en justificación que "*para satisfacer los requerimientos es necesario crear tokens biométricos basados en las fotografías*".

g) En el apartado 6, el número de sujetos en la respuesta pone, alto, más de 1000, y que la información es recogida en formato electrónico, online (6.3).

h) En el apartado 7.4, se indica que el período de almacenamiento de los datos es de hasta 5 años excepto los biométricos.

i) En el apartado 8 de integridad y confidencialidad se indica que los datos son almacenados en terceras partes siendo el formato en texto y en imágenes, y que el *token biométrico* está encriptado, se hacen copias de seguridad de los datos que se crean y mantienen, y existe huella de rastreo de los accesos a los datos, figurando los datos encriptados-

2) También es aportado el documento informe de DPIA, "*actualizado a 27/06/2022*", "*razones para la actualización: se refiere al anterior del sistema "one trust", usando ahora un formato diferente que comprende mas información*.

La parte A-información sobre el tratamiento proyectado, se estructura en 14 partes:

Primero responde a las cuestiones de la finalidad y de cómo funciona el sistema.

Para tratar dato biométrico obtenido del uso de tecnología de FR-reconocimiento facial- durante el proceso de registro para el evento antes de la asistencia y durante el control de acceso. "*El principal motivo para usar FR es asegurar que GSMA necesita un alto grado de seguridad junto al acceso sin contacto y vía rápida de acceso al evento para minimizar los riesgos de extender COVID 19*. *La tecnología utilizará la medición de puntos de la cara (distancia entre ojos o de la frente a la barbilla) para verificar la identidad de la persona a través de un modelo biométrico. Se tratan un numero de datos de puntos para crear un mapa de la cara de la persona en tiempo real. Esto se convierte en un modelo de plantilla seguro, usando un complejo algoritmo para crear el "token biométrico*". "*Para propósitos de seguridad en el acceso a la sede, GSMA cotejará automáticamente la imagen cogida en el punto de acceso contra el "token biométrico", almacenado en su base de datos. Están incluidos en el tratamiento terceras partes, SCAN VIS, el proveedor de la tecnología de FR. Los datos*

biométricos son obtenidos antes del evento, durante el registro. Aporta en anexo i un diagrama detallando el proceso de recogida de datos en el que figura que "*Para el registro se usa el software JEMEX REG SYSTEM que permite integración de terceras partes además de subir documentos, como en este caso, "el usuario ha de cargar el pasaporte" y el software una foto retrato, efectuando la comprobación de si la imagen es legible por el sistema.*

Los datos biométricos son almacenados en la Unión Europea en servidores de Amazon en Alemania y en España

La segunda cuestión es los datos de las personas que se recogen a nivel de categorías número de individuos y área geográfica.

La tercer cuestión es el tipo de datos que incluye la cuestión de porqué son solicitados, indicando que el pasaporte y los datos biométricos tienen la finalidad de "*confirmar la identidad y poder entrar al evento*". Siendo la fuente de origen "*las mismas personas*".

-Si se tratan datos de carácter especial, indicando que si, en dato biométrico "*ID verificación y control de acceso"*

5-"*proveedores de servicio*": se refiere a SCANVIS que gestiona el servicio FR, que proporciona una aplicación web "*incluida en el data exporter registration system and using this dieget data importer will help a data exporter to collect a quality verified fase phto/profile photo through the widget* . ScanVis está localizada en Hong Kong, algunos de sus empleados están localizados en China, pero están sujetos a las políticas de *ScanVis,* incluyendo la política de seguridad en la protección de datos.

"ScanVis ha contratado servidores de Amazon para el almacenaje de los datos biométricos que trata cuando proporciona servicios a la reclamada. Amazon actúa como un sub encargado. El acceso de ScanVis a los servidores de Amazon es remoto y esporádico, solo cuando hay un asunto técnico.
ScanVis puede acceder cuando hay un asunto técnico con las tokens biométricos.

6- "*otras revelaciones a terceras partes* " Se indica que cada año con anterioridad a la celebración del MWC, los *Mossos d`Esquadra*, envían una carta solicitando a la reclamada que proporcione información en relación con asistentes: nombre, apellido y número de pasaporte de los asistentes. Los datos biométricos no son compartidos con los Mossos d' Esquadra. La solicitud se lleva a cabo bajo un plan de seguridad el plan director de seguridad del Mobile World Congress, al cual no tienen acceso.

La séptima la información que se proporcionará a las personas
La octava los derechos individuales y las opciones
La novena, comunicaciones de marketing
La décima ,recogida automática de datos
La 11, período de retención
La 12, destrucción
la 13, seguridad
la 14, otros

La parte segunda se refiere a la metodología de la valoración del riesgo, dividida en parte b 1"*Metodología*" que parte de que "*una vez el riesgo ha sido identificado, es esencial calificar la probabilidad de que acontezca-probabilidad- así como el nivel de impacto que su materialización conlleva-severida*d. ""*Esta cuantificación depende de la descripción del tratamiento, las circunstancias y el medio en que se lleva a cabo*". Adjunta unos cuadros de color de probabilidad/severidad, con los valores muy bajo, bajo, medio, alto y muy alto

La parte b.2, "*dos*" " requisitos para llevar a cabo una DPIA", se divide en:

Obligación de presentar una DPIA
Valoración de la necesidad idoneidad y proporcionalidad del tratamiento

La parte b 3 "*evaluación de riesgo*", lleva una tabla en la que se indica: "*probabilidad- identificar la probabilidad de la materialización del riesgo identificado, considerando el tratamiento y las medidas tomadas por el diseño y el defecto*", constando en todas ellas bajo, o muy bajo, en "*severidad*" algunos apartados llevan "*alto*", el "riesgo resultante de combinar probabilidad y severidad", consta medio y bajo y la ultima, de: "*Identificar como el riesgo puede ser mitigado*", figurando que no es necesario o que se mitiga. Se subdivide en 23 apartados-no se citan todos-, destacando:

1-Responsabildiad del cumplimiento.
2-Roles en el tratamiento
3-DPO y representantes
4-Licitud
5-Avisos de información
6.Bases legitimadoras
7-Limitación de la finalidad
8-Calidad de datos y minimización
9-Retención de datos
10 Derechos de las personas
11- Toma de decisiones automáticas y perfiles
12- sin contenido
13-Seguridad
14- Exportación de datos
15-Cumplimiento con la política
20 privacidad por diseño y por defecto

Finaliza con un cuadro en una columna "*tipo de recomendación*", en la otra, "*recomendaciones*".

En tipo: "*Recomendaciones legales*", revisión del DPIA en un esquema anual considerando que los equipos legales monitoricen las retiradas del consentimiento, sus niveles, y el número de quejas y sugerencias que podría significar que no se ha entendido el lenguaje del consentimiento, estos son actualmente muy bajos. Revisar también la Política de Privacidad y las FAQS sobre el tratamiento de datos biométricos,

"*Recomendaciones organizacionales*": incluyen implementación de políticas, formación, y medidas de auditoría, En recomendaciones: para que se auditen los

derechos en el contrato de ScanVis y verifique el cumplimiento con el contrato, por ejemplo contemplando la provisión de la confirmación del borrado de datos por escrito al final del contrato, y llevar a cabo la verificación o monitorización de los empleados con las actuales políticas de Protección de Datos

"*Recomendaciones de producto*", definidas como las que requieren implementación técnica, medidas de anonimización , configuración del menú, notas contextuales, figura sin recomendaciones, y

"*otras recomendaciones*", que no se incluyan en las anteriores, no figura nada.

OCTAVO: Con fecha 20/12/2022, se formuló propuesta de resolución, con el literal:

"*Que por la Directora de la Agencia Española de Protección de Datos se sancione a* **GSMA LIMITED***, con NIF CIF* ***N4004237F*** *por una infracción del artículo 35 del RGPD, de conformidad con el artículo 83.4 a) del RGPD, y a efectos de prescripción en el artículo 73.t) de la LOPDGDD, con una multa de 200.000 euros*."

NOVENO: Con fecha 10/01/2023, tuvo entrada escrito de alegaciones en el que indica:

1) Menciona las Directrices 4/2022 del Comité Europeo de protección de Datos, CEPD "*European Data Protection Board* (EDPB), "*sobre el cálculo de las sanciones administrativas*", que figuran expuestas en la web *https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_es,* en *"periodo de consulta publica",* desde 16/05/2022 hasta 27/06/2022, sin que se hayan adoptado todavía. Manifiesta que en ellas se analizan detalladamente cada una de las circunstancias del artículo 83.2 del RGPD.

Indica que la propuesta no considera ninguna atenuante, y pide revisar y moderar la aplicabilidad de las circunstancias agravantes.

2) Solicita se consideren como atenuantes, con objeto de reducir el importe de la sanción:

2.1 "*El artículo 76.2.a) de la LOPDGDD establece como circunstancia a valorar el carácter continuado de la infracción. En el presente caso el tratamiento de datos objeto de la evaluación de impacto tuvo una duración muy limitada en el tiempo: concretamente se inició el día 22/03/2021, fecha en que se abrió el registro al MWC Barcelona 2021 ("Evento") donde se podía optar por el reconocimiento facial ("RF") y cesó cuatro semanas después de finalizado el Evento (el 29/07/2021), momento en que se suprimieron todos los datos biométricos recopilados. En total, el tratamiento de datos tuvo una duración de aproximadamente cuatro meses. Consideramos que se trata de una duración corta y que este hecho debe tomarse en cuenta como atenuante de la infracción."*

2.2. "*El artículo 76.2.f) de la LOPDGDD establece como circunstancia a valorar la afectación a los derechos de los menores. La naturaleza profesional y de netwo-*

rking del Evento hace que se dirija a personas adultas relacionadas con el ámbito de la tecnología. Estas personas tienen -previsiblemente- conocimientos tecnológicos por encima del ciudadano medio, y están especialmente capacitados para decidir por sí mismos si desean escoger la opción del RF como método de registro al Evento. En muy escasas ocasiones (por ejemplo, cuando un asistente no puede conseguir que alguien se quede al cuidado de su hijo) se gestionan datos de menores de edad. Los menores de edad se registran siguiendo un proceso por separado, como acompañantes, y quedan excluidos del sistema de registro por RF. Podemos confirmar que no se ha utilizado RF con ningún menor de edad. "

2.3. "*El artículo 83.2.e) RGPD establece como circunstancia a valorar toda infracción anterior cometida por el responsable o el encargado del tratamiento. Las Directrices 04/2022 consideran que se debe valorar la existencia de infracciones previas, atendiendo en especial a la temporalidad y a la materia de estas. Desde 2006 en que GSMA celebró por primera vez el Evento en Barcelona, no se ha registrado ninguna infracción de la normativa de protección de datos sancionada por la AEPD. Consideramos que, el hecho de que se trate de una primera infracción es especialmente relevante, teniendo en cuenta que GSMA lleva 16 años organizando eventos de grandes dimensiones en España y que, hasta el momento, nunca se ha cometido ninguna infracción, lo que demuestra el compromiso y la implicación de GSMA en lo referente al cumplimiento de la normativa en materia de protección de datos personales*"

2.4. "*El artículo 83.2.e) RGPD establece como circunstancia a valorar el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción. Desde GSMA se apuesta claramente por la transparencia y la colaboración con las administraciones públicas, en este caso concreto, GSMA ha estado a disposición de la AEPD y ha respondido a los requerimientos de información de la mejor manera posible, facilitando documentos e información relevante para el caso. Adicionalmente en este sentido, y sin que hubiera sido requerida por la AEPD, se ha facilitado información sobre la nueva evaluación de impacto realizada con la intención de cumplir con la normativa y corregir el incumplimiento en los eventos futuros*".

3. "*Sobre los agravantes de los artículos 83.2.a) y 83.2.b) RGPD que se aplican en la propuesta de resolución, solicitamos que se revisen y se valore su aplicabilidad en el caso concreto teniendo en cuenta los siguientes argumentos:*

3.1. La propuesta de resolución considera, sobre el agravante del artículo 83.2.a) RGPD, que "se trataron datos de un número muy elevado de asistentes (20.000 personas), sin contemplar el nivel de riesgo alto, en relación con la afectación a sus derechos y libertades, que puede existir para los tratamientos basados en reconocimiento facial". Sobre este aspecto corresponde indicar que el RF se ofrecía como medida opcional de registro y que, de acuerdo con la información proporcionada por nuestros sistemas de registro, el RF sólo fue utilizado por 7.585 personas. Solicitamos que se tenga en cuenta este número para la valoración del importe de la sanción. También corresponde indicar que no se ha tenido constancia, ni durante el tiempo que se realizó el tratamiento, ni con posterioridad, de que se produjeran daños o perjuicios o afectación alguna a los derechos y libertades de los interesados.

3.2. *La propuesta de resolución considera, sobre el agravante del artículo 83.2.b) RGPD, que no se tiene constancia de que la entidad haya obrado*

dolosamente, aunque la actuación revela una grave falta de diligencia en su conducta en la adopción de medidas proactivas precisas en un régimen tan singular, diferenciado y especial aplicable al tipo de datos que trata, sin que conste que se hayan puesto los medios básicos para que no se produjera. La actuación a la que hace referencia la propuesta de resolución es el propio incumplimiento del artículo 35 del RGPD. No se describen o relacionan circunstancias adicionales que puedan valorarse para justificar la aplicabilidad de este agravante. A este respecto, GSMA ha presentado información que demuestra diligencia en el tratamiento realizado, la aplicación de medidas de seguridad robustas impuestas a los proveedores de servicios de RF y la existencia de contratos adecuados con todos ellos. En este sentido, no estamos de acuerdo en que exista negligencia en la infracción y consideramos que la infracción del artículo 35 del RGPD, por sí sola, no puede conllevar la aplicabilidad del agravante de negligencia.

4-Finaliza indicando que: "*solicita que la AEPD reconsidere la propuesta de resolución y se proceda a dejar en apercibimiento o bien reducir la cuantía de la sanción*".

NOVENO: De las actuaciones practicadas en el presente procedimiento y de la documentación obrante en el expediente, han quedado acreditados los siguientes:

HECHOS PROBADOS

1) En los términos y condiciones de asistencia para el MOBILE WORLD CONGRESS (MWC) de Barcelona 2021, figura que GSMA Ltd. ('GSMA') es la entidad organizadora del MOBILE WORLD CONGRESS (MWC) de Barcelona 2021, a celebrar entre el 28/06 y el 1/07/2021 , y realiza entre otros, tratamientos de datos de los asistentes. La web www.mwcbarcelona.com/legal contiene información sobre el Congreso de Barcelona 2022, indica que "*GSMA LTD con su principal lugar de negocio localizado en Atlanta, USA, subsidiaria de propiedad entera de la asociación GSM, y con respecto a 4yfn 2022, GSMA 4fyn EVENT MANAGEMENT S.L., una subsidiaria de GSMA LTD., le da la bienvenida al MWC BARCELONA 2022.",* y que "*GSMA LTD y sus afiliados le proporcionan el evento*…" Según información de internet, GSMA (Global System for Mobile Communications, "*Sistema Global para Comunicaciones Móviles*), es una organización de la industria del móvil que agrupa a operadores de todo el mundo, mas de 750 operadores de telefonía móvil y mas de 400 Compañías están asociadas como miembros.
De acuerdo con la reclamada*: GSMA EVENT PROJECT MANAGEMENT, S.L. (EPM) es una filial española de GSMA. EPM se ha creado específicamente para prestar servicios relacionados con la gestión del MWC en Barcelona. Las actividades de tratamiento de datos personales de la GSMA están inextricablemente vinculadas a las actividades de EPM.*

Por lo tanto, la GSMA trata datos personales en el contexto de las actividades de un establecimiento de la UE y está sujeto al RGPD con arreglo al artículo 3, apartado 1 del RGPD, de modo que no se requiere ningún representante de la UE de conformidad con el artículo 27 del RGPD."

La citada entidad no figura inscrita en el Registro mercantil, si figurando: GSMC

EVENT PROJECT MANAGEMENT, S.L., cif B64828973 y como objeto social:" la prestación de servicios de gestión de proyectos, y de servicios de apoyo en relación con las conferencias congresos, espectáculos y reuniones organizados por cualquier de las sociedades pertenecientes al grupo de la sociedades pertenecientes al grupo"

Por otro lado la entidad GSMA 4YFN EVENT MANAGEMENT S.L, CIF ***B67299297***, domicilio Av. de la Reina Maria Cristina S/N Hall 1, Barcelona, tiene objeto social "*prestación de servicios de conferencias y eventos. organización de eventos empresariales, sociales, culturales, recreativos o tecnológicos, incluyendo puesta en marcha de ferias de muestras, etc.*". En la consulta a la aplicación AXESOR, figura como socio único GSMA LIMITED. A GSMA LIMITED le figura en la aplicación AXESOR como entidad no residente, el NIF ***N4004237F***

2) En los términos y condiciones de asistencia, se prevé el proceso de registro que posibilitaría el acceso presencial de los asistentes para el evento para ese 2021, se ha de crear una cuenta en su sitio web, y registrarse para la asistencia, de modo que al llegar a la sede física ya se debía estar registrado. En la sede no habría áreas de apoyo en el registro ni se proporcionarían credenciales impresas. El sistema pretendía tener una verificación de la identidad recogida antes de la llegada de cada persona a la sede. Para el año 2021, el MWC disponía como obligatorio en modalidad de asistencia presencial a su sede, el registro del DNI/ pasaporte, tarjeta de identidad, subiéndolo a su web. Solamente no era exigible subir los documentos identitarios a los que optaran por modalidad "*virtual*". Estos requisitos se contemplan en el Clausulado de "*términos y condiciones generales para la asistencia" MWC 2021, Barcelona*" en el que los asistentes tienen que aceptar dichas condiciones.

En los términos y condiciones de asistencia, se prevé *"Identificación: Usted acepta llevar una identificación con foto emitida por su gobierno en forma de pasaporte o tarjeta de identificación nacional de la UE con usted en todo momento durante el Evento. Se le pedirá que presente dicha identificación. Usted es el único responsable de la exactitud de todos los datos personales proporcionados al registrarse para el Evento*…"
Además, se recogen en el registro de los usuarios, datos como "*nombre, cargo, nombre de la empresa, dirección trabajo, email de trabajo, funciones laborales, número de teléfono, área de interés y fotografía. Si eres un ponente, como información adicional, tu perfil profesional"*

3) La reclamada indicó a la reclamante que el pasaporte y los datos de identificación se requieren y son exigidos por los *Mossos d`Esquadra*, que la base legitimadora para el tratamiento de la subida de los pasaportes y tarjetas de identidad es el artículo 6.1 c) del RGPD por cuanto se les exigió que facilitarán determinada información a los Mossos: nombre apellidos nacionalidad fecha de nacimiento documento de identidad facilitados fecha de expedición y número de documento, siendo esta manera de proporcionarlo novedosa, por ser electrónica y "*que ha cambiado para 2021, debido a que los negocios necesitan entorno sin contacto*". La reclamada no acredita esta exigencia ni que lo deba ser a través de una web, de su propia titularidad privada, donde se recogen y almacenan. Señaló la reclamada que en las anteriores ediciones del Congreso, los asistentes llevaban sus tarjetas identificativas en una credencial.

4) En términos y condiciones generales para los asistentes se indica en privacidad y

Protección de Datos que se recogen datos "*sobre ti en relación con la provisión de los servicios y para la administración de la cuenta" y* que más detalles sobre la política de práctica sobre el tratamiento de datos personales está disponible en *Política de Privacidad.* En Política de Privacidad se indica que se obtiene información sobre los datos recabados de diversos colectivos, entre otros, los asistentes, a través del sistema de registro de asistentes , la app del evento, tarjetas credenciales digitales y/o impresas, o el sistema de escaneo de reconocimiento facial (en los puntos de acceso, para sesiones o para participar en reuniones de espacios cerrados). Se indica: "información que proporciona voluntariamente: *"cuando… creas una cuenta con nosotros, te registras para el evento, ...requieres un servicio…""La información recogida incluye, pero no se limita a: tu nombre, cargo, nombre de la empresa, dirección trabajo, email de trabajo, funciones laborales, número de teléfono, área de interés y fotografía. Si eres un ponente, como información adicional, tu perfil profesional"*

5) La reclamada explica que a partir de la toma de los citados documentos identitarios, existe la posibilidad cuando se registra en la web, para el acceso presencial, de dos modos, y uno mas residual:

a) Reconocimiento de verificación automático, se denomina también validación de identidad automática: Junto a los documentos identitarios ya subidos, el programa de la web de la reclamada solicita el consentimiento expreso para usar BREEZ (siglas de entrada fácil con reconocimiento biométrico) que utiliza el reconocimiento facial biométrico . En esta modalidad se puede inscribir tanto durante el registro como después de haberse registrado para el evento .El sistema BREEZ supone que el software de *SCANVIS* -encargada del tratamiento de la reclamada- realiza una foto de la persona hace coincidir automáticamente la imagen "*que nos proporciona con la fotografía en su pasaporte/tarjeta nacional de identidad", "*a los que atribuirá unas puntuaciones de coincidencia", "l*a tecnología analiza los rasgos faciales, tomando medidas de los puntos de datos* que componen la cara, como distancia entre ojos, o de la frente a la barbilla, se *procesan una serie de puntos de datos para crear un mapa de su cara en tiempo real, esto se convierte en un patrón de datos utilizando un algoritmo para crear el que la reclamada llama "token biométrico",* (ficha biométrica, identificador). Ese token es el que posibilita que en los accesos su imagen captada por el lector de FR coincida y se acceda al evento en colas propias diferenciadas, para sesiones o para participar en reuniones de espacios cerrados o incluso áreas restringidas.

En los accesos sin contacto con BREEZ, se indica que "*verificará su imagen capturada por las cámaras contra su token biométrico para finalidades de validación de identificación*".

En la información del consentimiento en BREEZ se indica que "*Usted consiente para GSMA usando sus datos biométricos obtenidos de las fotografías proporcionadas por usted para finalidades de validación de identificación en el contexto del registro online y para el MWC Barcelona con finalidades de acceso a la sede",* precedido por una casilla que indica *"Si, consiento el uso de mis datos biométricos para la validación automática de identidad*".

Fundamenta la finalidad en un doble sentido, verificar la identidad cuando asiste al evento, y seguridad en el acceso al recinto. La base jurídica de este tratamiento según

indican sería el consentimiento expreso, pudiendo retirar su consentimiento con lo que su validación pasaría a ser manual.

La información sobre el sistema BREEZZ se amplia en la sección *BREEZ FAQS -FR*
El consentimiento otorgado para la validación automática de la identidad se puede retirar en cualquier momento

a) Reconocimiento de verificación manual, o validación manual de la identidad: Junto a los documentos identitarios ya subidos, el programa de la web de la reclamada realiza una foto de la persona asistente. Implica que el acceso se va a producir con control a través de presencia humana, que efectúa la verificación cuando el asistente al acercarse, escanea su credencial digital en forma de QR de lectura, mostrando la foto tomada que ve la presencia humana al mismo tiempo que a la persona.

b) Excepcionalmente, la validación de identificación en papel, presencial in situ
2) El denominado por la reclamada: "*token biométrico*" creado para el proceso de comparación de imágenes se eliminará cuatro (4) semanas después de la finalización del evento. Señala el apartado ¿cómo se utiliza y almacena en mis datos biométricos? que cada token biométrico se cifra y almacena en una base de datos separada de los datos sin procesar utilizados en su creación

No obstante en las FAQS de BREEZ se indica que a pesar de que no tiene contacto, todos los asistentes deben tener su credencial digital disponible para ingresar al perímetro externo del lugar y que la credencial digital también será la única forma de acceder a conferencias y sus sesiones de socios.

3) De acuerdo con la reclamada, la entidad *SCANVIS con la que tiene un encargo de* tratamiento del sistema de reconocimiento facial para el acceso a la sede, se encuentra en un país fuera de la UE*, y* GSMA ha suscrito cláusulas contractuales estándar con *SCANVIS*. Añade que los datos del MWC FR están alojados por Amazon Web Services («AWS») en Alemania.

4) La reclamada manifestó que en el MWC 2019, permitió que las copias en papel de los documentos de identificación se verificarán manualmente al acceder a la sede de MWC, opción que en 2021 se suprimió-salvo excepciones- por razones de salud y seguridad, con el fin de minimizar el riesgo de propagación *de la COVID*-19, reduciendo colas y las multitudes en los puntos de acceso. Esto está en consonancia con el "*plan de acción de congresos de la Generalitat de Cataluña*" al que está sujeto a la GSMA y que exige expresamente la sustitución de procesos manuales por procesos digitales.

5) Según la reclamada al MWC 2021, asistieron aproximadamente 20.000 personas.

10) Antes del MWC de 2021, la reclamada disponía de un documento de EVALUACION DE IMPACTO que es aportado en alegaciones, titulado: "*MWC20 Facial recognition process",* creado el 17/12/2019. Tiene nueve apartados con respuesta si/no, relacionados con los principios de protección de datos, figurando cero en toda clase de riesgos, riesgo residual, ninguno. En varias cuestiones reproduce el artículo del RGPD, y la respuesta: Si (ejemplo 4.5, 4.4, 4.6 entre otros) En el primer

apartado: "*general*", se indica que "*es una nueva versión del proceso de reconocimiento facial actualizado para el 2020*" (en el se mencionan eventos fechados en el Congreso de 2020, ninguno de 2021), y que el "*termino BREEZ es el término orientado al cliente para nuestro proceso de reconocimiento facial*". Es una revisión del proyecto de 2019, en la que se incluyen sus cambios desde entonces, refiriendo el funcionamiento de BREEZ. En el apartado de ¿Cómo valorarías la importancia de la necesidad de las operaciones de tratamiento*?* (5.2) no se indica la actividad de tratamiento del reconocimiento facial, indicando: " *Con el fin de satisfacer las medidas de seguridad en el evento, hemos sido instruidos por el Formulario de la Policía Española para poner en marcha procesos estrictos para garantizar que todos los asistentes sean examinados a través de una verificación de pasaporte/documento de identidad de la UE antes de que puedan ingresar en el recinto, y recoger sus credenciales. Los procesos heredados se basan en verificaciones manuales que pueden ser lentas y brindar una experiencia negativa en el evento. A través del uso de la tecnología descrita en este DPIA, podemos automatizarlos para permitir un uso mucho más proceso eficiente, así como un evento más preciso y seguro*."

En el apartado 5.3 sobre la proporcionalidad de las operaciones de tratamiento solo se indica que si, "*para satisfacer los requerimientos, es necesario crear tokens biométricos basados en las fotografías*". El documento carece de evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad; el uso del reconocimiento facial para el acceso a los eventos, de su evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, del artículo 35 del RGPD y de las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el RGPD, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas. Igualmente, relaciona los datos de los pasaportes y tarjetas de identidad que manifiesta son exigidos por los *Mossos d`Esquadra* que presuntamente tienen una finalidad, para conectarlo con la foto que se hacen con el software, que inicia el proceso de reconocimiento facial, emparejando su identidad para facilitar el acceso.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento 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

De acuerdo con los términos en que se formula la reclamación, siempre es obligatorio antes de acudir presencialmente al Congreso, su sede y sus eventos, registrarse en la web de la reclamada, de modo que cuando se llegue se debe estar ya registrado. Ello se lleva a cabo con la creación de una cuenta y el registro en la web de la reclamada. Es obligatorio en general, cuando se asista presencialmente el registro en la web con la introducción en dicha web, en forma de subida del documento (DNI, o pasaporte, por motivos de seguridad exigido según la reclamada por los Mossos d`Esquadra, y de una foto por motivos de identificación en los accesos del evento, , documentos de identificación, que el año anterior se presentaban o exhibían, este 2021 se suben a la web y se hacen en la web.

Valora la reclamada que la subida a su web de dicha documentación identitaria (DNI y o pasaporte documento identificativo) le es exigida por los Mossos d`Esquadra, incluido en el artículo 11.1.h) de la Ley 2/1986, de 13/03, de Fuerzas y Cuerpos de Seguridad, que indicaría:

"*1. Las Fuerzas y Cuerpos de Seguridad del Estado tienen como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana mediante el desempeño de las siguientes funciones.*
[…]"

a) *Captar, recibir y analizar cuantos datos tengan interés para el orden y la seguridad pública, y estudiar, planificar y ejecutar los métodos y técnicas de prevención de la delincuencia*"

Este requerimiento en el tratamiento de datos, no se ha analizado en concreto en este procedimiento, pero si se indica por la reclamada que para este 2021, este proceso ha cambiado, "*proporcionándose electrónicamente*", "*por el entorno sin contacto*". Parece ser que en otros años se mostraban estos documento al acceder al recinto, limitando en parte la intrusión que el tratamiento de estos datos les supone a sus titulares el tener que subirlos a una web titularidad de la reclamada. En 2021 era obligatorio, no pareciendo que por conveniencia se puedan recabar datos que podrían ser excesivos, cuando antes cabía una mera exhibición del documento, máxime tratándose de documentos oficiales de identificación, que como bien se instruye, además, "*han de portar las personas en todo momento*"

Tampoco está claro como traslada los datos identificativos que recoge de cada asistente la reclamada a los Mossos d`Esquadra, si entrega el documento identificativo que los asistentes suben a la web de la reclamada y la foto, o sólo dan los datos que precisa, lo que la obligaría bien a extraerlos uno a uno por personas dedicadas a ello. Al intentar promover el no contacto por la pandemia, en vez de exhibir el documento, la reclamada se queda con un ejemplar del mismo.

En todo caso, la reclamada debería reevaluar si dispone de una legitimación para esta actividad de tratamiento.

Al asistente al Congreso, además, se le entrega una credencial o tarjeta digital que contiene sus datos. Al asistente en modo virtual, no presencial, no se le exigía la identificación previa en forma de aportar DNI, documento de identificación o pasaporte.

La modalidad común de registro en cuanto al acceso es la validación manual, que partiendo de la subida de los citados documentos, y la foto, no aplica reconocimiento facial. La persona que asiste el evento accede llevando su credencial que porta y muestra y escañándola, un empleado verifica que la persona que accede coincide con la de la fitografía y los documentos que lleva en las credenciales

Otra modalidad de registrarse y acceder, supone introducir los mismos datos, pero prestando el consentimiento, marcando una casilla para ello, que asociaría los mismos documentos para una modalidad de entrada fácil, mediante el reconocimiento biométrico facial. Esta identificación se produce, no solo por introducir el documento publico de identificación de la persona en la web como forma de identificarse, que en si no es un dato biométrico, sino partiendo de una foto que hace el software, que compara con la foto del documento de identidad-pasaporte, y después de llevarse a cabo un tratamiento técnico especifico: transformación mediante un algoritmo sobre los puntos del rostro, convirtiéndolos en plantilla, o *token biométrico*, como lo denomina la reclamada.

De este modo, con el pasaporte, o DNI, como obligatorio, sin alternativa, mas el reconocimiento facial, se procede en forma bivalente a una identificación con doble factor conjunto, usando el reconocimiento facial para acceder de forma sin contacto y mas ágil a la instalación. Se asegura que es esa persona por los documentos subidos a la web y por la plantilla biométrica que gestiona la misma web de la reclamada a través de un encargado de tratamiento.

Por otro lado, en los tratamientos sin reconocimiento facial, también se está guardando la foto, que se desconoce si se gestiona también por *SCANVIS* en su programa que está en la web de la reclamad, y si se hace algún emparejamiento con el pasaporte/DNI en orden a verificar umbrales de coincidencia para deducir la identificación del asistente que entra en modo manual portando su credencial.

La reclamante parece englobar cualquier acceso físico como ligado a los datos biométricos y su uso. Sin embargo, pese a que manifiesta que si que tuvo que subir el pasaporte, no acredita el uso de los datos biométricos, y la reclamada asevera que no utilizó dicha modalidad, señalando que "*se registró como asistente virtual y tomó parte como orador en una mesa redonda*" y "*no se le solicitó descargar o subir documento de identidad*".

III

El ámbito de aplicación del RGPD extiende su protección, tal y como establece su artículo 1.2, a los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales, definidos en su artículo 4.1 como "*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*."

La reclamada ha tratado datos de carácter personal, y específicamente datos biométricos. El concepto de tratamiento El RGPD define en su artículo 4:

"*2) «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;*

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

Los datos biométricos como tipos específicos los define el artículo 4.14 del RGPD:

" 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;

Las categorías especiales de datos a que se refiere el artículo 9 del RGPD, establece:

"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."

En este caso a los que consentían el uso del reconocimiento facial, se les tomaba una fotografía por el programa sobre el que se produce el tratamiento técnico especifico que finaliza en la creación de la plantilla biométrica mediante la aplicación de un algoritmo.

Así pues, la información biométrica recogida (por ejemplo, la imagen de una huella dactilar) se procesa siguiendo procedimientos definidos en estándares, y el resultado

de ese proceso se almacena en registros de datos denominados firmas, patrones o "*templates*". Estos patrones registran numéricamente las características físicas que permiten diferenciar personas, son datos de la persona, no sobre ella, constituyen una forma de representación matemática reducida de la característica original. Expresan de forma univoca y compacta la identidad del individuo. No se almacena los datos brutos sino un extracto de sus características.

El patrón biométrico extraído por el módulo de inscripción es almacenado en la base de datos del sistema de reconocimiento. El patrón biométrico se almacena para su comparación. La base de datos contendrá, por tanto, todos los patrones biométricos de los individuos que sean usuarios legítimos del sistema. También, dependiendo de la aplicación, podría almacenarse dicho patrón **sobre otros soportes** como, por ejemplo, una tarjeta magnética o una tarjeta inteligente (técnicas match-on-card y match-on-token). En estos casos, los datos se almacenan exclusivamente sobre el soporte tarjeta, no existiendo una base de datos centralizada.

El sistema de datos biométricos, en el proceso de identificación o verificación no busca una eventual igualdad entre la muestra y el dato almacenado, sino que tiene como objetivo encontrar los suficientes puntos coincidentes para determinar que existe una coincidencia, no la igualdad. Así lo reconoce la reclamada al indicar que se coteja la foto que se hace con la del pasaporte, estableciendo un umbral de coincidencias alto para continuarse el proceso en la creación de la plantilla.

En la última fase del proceso, se comparará una muestra biométrica-como la cara-presentada al sensor con un patrón que figura en la base de datos de la reclamada.

La definición de datos biométricos incluye que a través del tratamiento técnico especifico, "*permitan o confirmen*" "*la identificación única*" de dicha persona. Las menciones a "*permitan*" pueden entenderse a la identificación, la de "*confirmen*" a la verificación. Por tanto, ambas, identificación o autenticación han de ser únicas, referidas a la identificación que se produzca de la persona . La identificación única por otro lado, va mas allá de que el dato sea de una persona física identificada o identificable. Dato de persona física identificada es que esa persona se la distingue o aísla de un grupo de personas. Único, puede referirse a que los datos biométricos tienen tales particularidades que pueden identificar sin ambigüedades a un individuo

En el presente caso, desde luego, no puede hablarse de que no se trata información ligada a datos personales de una persona identificada en cada acceso a la sede en modo presencial, aunque los datos se guarden en el dispositivo cifrados/encriptados. Cada vez que un asistente se sitúa en los aledaños del acceso, frente al espectro que alcance la cámara, permite o confirma su identificación única a través del tratamiento que lleva a cabo la reclamante con los dispositivo adquiridos y mediante la tecnología de software implantada. La muestra presentada se compara y el sistema tiene la función de identificación con una función biométrica, identificando únicamente al asistente que dice ser y registrando sus datos.

Los datos biométricos presentan la particularidad de ser producidos por el propio cuerpo y lo caracterizan definitivamente, son datos no sobre esa persona, sino que los datos refieren a la misma persona, en principio no modificables por voluntad del individuo, ni la persona puede ser liberada de ellos, no se pueden cambiar en caso

de compromiso-pérdida o intrusión en el sistema. Además, debido a que los datos biométricos son propios de una persona y perpetuos, el usuario utiliza los mismos datos en diferentes sistemas. Por lo tanto, un robo de identidad no solo es perpetuo en el tiempo, sino que afecta a todos los sistemas en que un usuario tenga almacenados sus datos biométricos. El titular por lo tanto, no tiene la posibilidad de utilizar un dato biométrico para el banco, y uno diferente para su sistema de salud, sino que utiliza la misma información para verificar su identidad en ambos, y frente a una vulnerabilidad se ven afectados todos ellos al mismo tiempo. Finalmente, el interesado no se entera de que su información está siendo utilizada, pudiéndose obtener a través de objetos, rastros o cámaras de vigilancia.

Los considerandos 51 y 75 del RGPD se refieren a los datos espaciales, "un grupo de datos personales que, por su naturaleza, son particularmente sensibles por razón del importante riesgo que pueden entrañar, en el contexto de su tratamiento, para los derechos y libertades fundamentales. El común denominador de todos ellos es que su tratamiento comporta un *riesgo importante* para los derechos y las libertades fundamentales ya que puede llegar a provocar daños y perjuicios físicos, materiales o inmateriales. En este grupo o categoría de datos *particularmente sensibles* se incluyen las categorías de datos especialmente protegidos que regula el artículo 9 del RGPD -considerando 51 del RGPD- y, además, otros muchos datos no regulados en ese precepto. El considerando 75 menciona con detalle los datos personales cuyo tratamiento puede entrañar un *riesgo, de gravedad y probabilidad variables*, para los derechos y libertades de las personas físicas como consecuencia de que pueden provocar daños y perjuicios físicos, materiales o inmateriales. Entre ellos menciona aquellos cuyo tratamiento "*pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo;"* (El subrayado es nuestro)

El considerando 51 del RGPD se refiere a la no consideración sistemáticamente como un tratamiento de categoría especial de datos, a las fotografías, a menos que se les aplique un medio de tratamiento técnico especifico que "*permita la identificación o la autentificación unívocas de una persona física*".

Se denominan de esa manera porqué su tratamiento implica situaciones en las que surge un riesgo grave de protección de datos, desde las consecuencias de que su uso indebido puede tener para las personas, y se consideran tan perjudiciales que su tratamiento está prohibido a menos que se aplique una excepción, en este caso el consentimiento expreso.

Además de darse la circunstancia que levante en su caso la prohibición de tratamiento, debe concurrir alguna de las bases legitimas para que el tratamiento de datos sea lícito, que se definen en el artículo 6.1 del RGPD, y cumplir con los principios que se expresan en el artículo 5 del RGPD, entre los que juegan importante papel la minimización y proporcionalidad y necesidad de tratamiento de esos datos.

En este caso se alude a la base del consentimiento para levantar la prohibición de tratamiento, existiendo además según declara la reclamada, la opción de no uso del sistema de FR, sin sufrir restricciones en accesos.

IV

El artículo 7 de la Carta de Derechos Fundamentales de la Unión Europea, proclamada por el Parlamento Europeo y el consejo de la Unión Europea y la Comisión de 7/12/2000, prescribe que toda persona tiene derecho al respeto a su vida privada, y el artículo 8.1 que toda persona tiene derecho a la protección de datos de carácter personal que le conciernen. Interpretadas conjuntamente, se infiere que puede constituir una vulneración de tales derechos cualquier tratamiento de datos por parte de un tercero, en este caso la reclamada. Esta utilización de los datos de las personas que asisten al evento por ella organizado, bajo sus condiciones en las que establece el medio y el fin por el que lleva a cabo el tratamiento de datos, supone una intromisión de su derecho a la vida privada y a la protección de datos si no resultara justificada. El artículo 8.2 de la Carta de Derechos fundamentales precisa que los datos de carácter personal solo pueden ser tratados con el consentimiento del interesado o en virtud de otro fundamento legitimo previsto por Ley. Además, los artículos 7 y 8 de la carta no son absolutos, admitiendo limitaciones, siempre que estén previstas por la Ley, respeten el contenido esencial de esos derechos y con observancia del principio de proporcionalidad, sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás (Sentencia del Tribunal de Justicia de la Unión Europea, sala cuarta, sentencia de 15 de octubre del 2013, C/291/2012.). Estos aspectos por lo demás, se reiteran en relación con los derechos fundamentales, en el art. 52.1 *in fine* de la Carta de los Derechos Fundamentales de la UE

El tratamiento de reconocimiento facial presenta altos riesgos para los derechos y libertades fundamentales y antes de implantar un proyecto de tratamiento de datos, siempre y cuando sea probable que el mismo suponga un riesgo significativo para los derechos y libertades de las personas, es preciso auditar su funcionamiento, no de forma aislada sino en el marco del tratamiento concreto en que se va a emplear. Dadas las consecuencias potencialmente perjudiciales para las personas afectadas, deberán cumplirse requisitos más rigurosos en el proceso de evaluación de impacto de cualquier medida que interfiera con la dignidad de una persona, en términos de cuestionamiento de la necesidad y proporcionalidad, así como de las posibilidades de los individuos para ejercer su derecho a la protección de datos

Así se dictamina en:

- El apartado 72, de las Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de video, de 29 de enero del 2020, del CEPD, indica: "*El uso de datos biométricos y, en particular, del reconocimiento facial conllevan elevados riesgos para los derechos de los interesados. Es fundamental que el recurso a dichas tecnologías tenga lugar respetando debidamente los principios de licitud, necesidad, proporcionalidad y minimización de datos tal y como establece el RGPD. Aunque la*

utilización de estas tecnologías se pueda percibir como particularmente eficaz, los responsables del tratamiento deben en primer lugar evaluar el impacto en los derechos y libertades fundamentales y considerar medios menos intrusivos de lograr su fin legítimo del tratamiento. " Es decir, habría que responder la cuestión de si esta aplicación biométrica es algo que realmente es imprescindible y necesaria, o es solo "*conveniente*".

-El Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, del GT 29, establece que "*Independientemente de la base jurídica de dicho tratamiento, antes de su inicio se debe realizar una prueba de proporcionalidad con el fin de determinar si el tratamiento es necesario para lograr un fin legítimo, así como las medidas que deben adoptarse para garantizar que las violaciones de los derechos a la vida privada y al secreto de las comunicaciones se limiten al mínimo*

Desde que en los años 90 del pasado siglo nuestro Tribunal Constitucional adoptó el denominado "*test alemán*" en el examen del principio de proporcionalidad, es una constante en su jurisprudencia, que las medidas que afecten a derechos fundamentales, deben ser idóneas o adecuadas, necesarias y proporcionadas en sentido estricto.

-El Grupo de Trabajo del artículo 29, GT29 (adoptado el 8/06/2017) (creado en virtud del artículo 29 de la Directiva 95/46/CE, órgano consultivo independiente europeo en materia de protección de datos y derecho a la intimidad, cuyos cometidos se describen en el artículo 30 de la Directiva95/46/CE y en el artículo 15 de la Directiva 2002/58/CE, asumidos hoy día por el Comité Europeo de Protección de Datos, CEPD), en su Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, indica que "Al analizar la proporcionalidad de un sistema biométrico propuesto, es preciso considerar previamente si el sistema es necesario para responder a la necesidad identificada, es decir, si es esencial para satisfacer esa necesidad, y no solo el más adecuado o rentable. Un segundo *factor que debe tenerse en cuenta es la probabilidad de que el sistema sea eficaz para responder a la necesidad en cuestión a la luz de las características específicas de la tecnología biométrica que se va a utilizar. Un tercer aspecto para ponderar es si la pérdida de intimidad resultante es proporcional a los beneficios esperados. Si el beneficio es relativamente menor, como una mayor comodidad o un ligero ahorro, entonces la pérdida de intimidad no es apropiada. El cuarto aspecto para evaluar la adecuación de un sistema biométrico es considerar si un medio menos invasivo de la intimidad alcanzaría el fin deseado".*

Estas valoraciones requieren exhaustividad, partiendo en este caso, no solo de la prohibición de tratamiento de estos datos, sino considerando los riesgos de usar una tecnología intrusiva, los sesgos o la probabilidad de un error en la identificación, su interoperabilidad, la suplantación de la identidad y el tipo de identidad única, permanente e invariable que se tratan, su impacto en la privacidad de las personas, las implicaciones en cuestión de derechos fundamentales de tales sistemas y las medidas de seguridad, Su uso cada vez más extendido, e interconexión tecnológica es más probable que interfiera con estos derechos fundamentales y puede dar lugar a vulneración grave de derechos.

Los responsables del tratamiento deben garantizar que la evaluación de la necesidad y la proporcionalidad considere una evaluación exhaustiva de las opciones alternativas menos intrusivas disponibles. Por consiguiente, se ha de documentar la viabilidad de otras opciones alternativas disponibles que no requieran el uso de datos especiales, comparar todas las opciones y documentar las conclusiones. Todo ello, considerando el contexto del marco en el que se traza el tratamiento, el cumplimiento de las obligaciones a través del registro de jornada.

La necesidad implica que se requiere una evaluación combinada, basada en hechos, sobre la eficacia de la medida para el objetivo perseguido y sobre si resulta menos intrusiva en comparación con otras opciones para lograr el mismo objetivo

La necesidad no debe confundirse con utilidad del sistema. Puede que se facilite el no tener que llevar una tarjeta, es automático e instantáneo y no excesivamente costoso. Obviamente, un sistema de RF puede ser útil, pero no tiene por qué ser objetivamente necesario (siendo esto último lo que realmente debe estar presente). Como establece el dictamen 3/2012 sobre la evolución de las tecnologías biométricas- del GT 29-, debe examinarse "*si es esencial para satisfacer esa necesidad, y no solo el más adecuado o rentable".* En cuanto a la fiabilidad del sistema, hay que decir que cuanto mayor sea el numero de sistemas de identificación que se basan en datos biométricos o en una plantilla obtenida a partir de datos biométricos, mayor es el riesgo de que este dato pueda acabar siendo utilizado de manera inadecuada y dando lugar a un riesgo de usurpación o suplantación de identidad.

El sistema de responsabilidad proactiva implantado por el RGPD, enfocado a la gestión continua de los riesgos potenciales asociados al tratamiento, impone a los responsables del tratamiento que analicen que datos tratan, con que finalidades y que tipo de tratamientos llevan a cabo, relacionando los potenciales riesgos a que están expuestos y a partir de ahí, decidir que medidas toman y aplican para asegurar su cumplimiento en función
de los riesgos detectados y asumidos.

La evaluación de impacto en la protección de datos personales, EIPD, es la herramienta que en el RGPD se ocupa de la garantía de cumplimiento de esta vertiente del tratamiento.

En el texto del RGPD no aparece una definición para el término "evaluación de impacto relativa a la protección de datos" o EIPD. El CEPD sí desarrolla la definición de EIPD en las **Directrices WP248** como: "… *un proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales evaluándolos y determinando las medidas para abordarlos*." Según esto, el CEPD considera que la EIPD, es un "*proceso*" y, por tanto:

• Reducir la EIPD a una actividad puntual y aislada en el tiempo es incompatible con el concepto de proceso que interpreta las Directrices WP248.

• La EIPD ha de estar documentada, pero la EIPD es más que el informe que refleja sus resultados.

• La EIPD ha de evaluar los riesgos "*determinando las medidas para abordarlos*". La EIPD obliga al responsable a actuar y tiene una dimensión mayor que un mero formalismo plasmado en un documento sobre el que se puedan realizar cambios mínimos para adaptarlo a cualquier tratamiento.

La EIPD es un proceso de análisis de un tratamiento que se extiende en el tiempo, a lo largo de todo el ciclo de vida de un tratamiento de datos personales, y que se ha de revisar de forma continua, "*al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento*" (art.35.11 del RGPD).

La reclamada no aporta dicho documento antes del inicio del procedimiento, y una vez aportado se estima que no cumple los mínimos requisitos que ha de contener , por lo que se le imputa la infracción del artículo 35 del RGPD, que señala:

"*1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.*

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o
c) observación sistemática a gran escala de una zona de acceso público.

4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.

5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.

6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de

control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

7. La evaluación deberá incluir como mínimo:
a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;
b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y
d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento."
En desarrollo del párrafo 4, la Directora de la AEPD aprobó un listado no exhaustivo, orientativo de los tipos de tratamiento que requieren una evaluación de impacto relativa a la protección de datos, indicándose: "*En el momento de analizar tratamientos de datos será necesario realizar una EIPD en la mayoría de los casos en los que dicho tratamiento cumpla con dos o más criterios de la lista expuesta a continuación, salvo que el tratamiento se encuentre en la lista de tratamientos que no requieren EIPD a la que se refiere en artículo 35.5 del RGPD*.

"*4. Tratamientos que impliquen el uso de categorías especiales de datos a las que se*

refiere el artículo 9.1 del RGPD … o deducir información sobre las personas relacionada con categorías especiales de datos.

5. Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física."

En este caso, se trata de la oferta de servicios a los asistentes a un Congreso, estableciendo un mecanismo de identificación que posibilite el acceso sin contacto basado en reconocimiento facial con la toma de la plantilla de su cara que se gestiona en un programa informático cuyo servicio es ofrecido por un tercero con el que se suscribió un contrato de encargo.

La obligación de realizar una evaluación de impacto en este supuesto, obedece a que"*utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas"*

En este caso, se han de analizar los riesgos diversos que se pueden dar, incluyendo su tecnología, en el marco de un uso cada vez más intensivo de este tipo de datos. Su uso, interoperabilidad e interconexión tecnológica, es más que probable que interfiera con estos derechos fundamentales y puede dar lugar a cuestionamientos sobre su implantación.

La utilización de datos biométricos y, en particular, el RF entraña mayores riesgos para los derechos de los interesados. Es fundamental que el recurso a esas tecnologías se haga respetando debidamente los principios de legalidad, necesidad, proporcionalidad y minimización de los datos establecidos en el RGPD. Si bien el uso de estas tecnologías puede percibirse como particularmente eficaz, los responsables deben, en primer lugar, evaluar el impacto en los derechos y libertades fundamentales y considerar medios menos intrusivos para lograr su objetivo legítimo del tratamiento.

La "*aproximación basada en el riesgo"* se desarrolla en el "*Statement on the role of a risk-based approach in data protection legal frameworks WP218*" del GT 29, WP218, y no es un concepto novedoso en el marco de la protección de datos.

La gestión del riesgo para los derechos y libertades, tiene por objetivo el estudio del impacto y la probabilidad de causar daño a las personas, a nivel individual o social, como consecuencia de un tratamiento de datos personales. Por el contrario, la gestión de riesgo de cumplimiento normativo tiene por objetivo facilitar al responsable una herramienta para verificar el grado de cumplimiento de las obligaciones y preceptos exigidos legalmente con relación a una actividad de tratamiento. Por lo tanto, previamente al proceso de gestión de riesgos y como condición sine qua non para emprender una actividad de tratamiento, es preciso sistematizar la verificación de cumplimiento normativo a lo largo de todo el ciclo de vida del tratamiento. La complejidad del proceso de gestión de riesgo ha de ajustarse, no al tamaño de la entidad, la disponibilidad de recursos, la especialidad o sector de la misma, sino al posible impacto de la actividad de tratamiento sobre los interesados y a la propia dificultad del tratamiento.

Como potencial fuente de riesgos, el conocimiento de las tecnologías que se pretenda utilizar, así como sus riesgos asociados, deben ser entendidos como una obligación

del responsable y parte de su deber de diligencia con relación al cumplimiento de las previsiones del RGPD.

El tratamiento biométrico presenta, entre otros los siguientes riesgos, algunos de los cuales se contemplan en el Dictamen 3/2012 sobre la evolución de las tecnologías biométricas del GT 29 de 27/04/2012:

-La definición del tamaño (cantidad de información) de la plantilla biométrica es una cuestión crucial. Por una parte, el tamaño de la plantilla debe ser lo bastante grande para gestionar la seguridad (evitando solapamientos entre los diferentes datos biométricos, o sustituciones de identidad), y por otra, no deberá ser demasiado grande a fin de evitar los riesgos de reconstrucción de los datos biométricos

-Riesgos que conlleva la utilización de datos biométricos para fines de identificación en grandes bases de datos centralizadas, dadas las consecuencias potencialmente perjudiciales parar las personas afectadas.

-No hace falta decir que toda pérdida de las cualidades de integridad, confidencialidad y disponibilidad con respecto a las bases de datos sería claramente perjudicial para cualquier aplicación futura basada en la información contenida en dichas bases de datos, y causaría asimismo un daño irreparable a los interesados. Por ejemplo, si los datos registrados de una persona autorizada se asociaran con la identidad de una persona no autorizada, esta última podría acceder a los servicios de que dispone el propietario del dato, sin tener derecho a ello. El resultado sería un robo de identidad, que (independientemente de su detección) quitaría fiabilidad al sistema para futuras aplicaciones y, en consecuencia, limitaría su libertad.

- La transferencia de la información contenida en la base de datos.

-Se puede crear la ilusión de que la identificación a través de la cara siempre es correcta, por ello se debe incluir un análisis de los errores que se pueden producir en su uso, medidores de evaluación del rendimiento, tasa de falsa aceptación-probabilidad de que un sistema biométrico identifique incorrectamente a un individuo o no rechace a un individuo que no pertenece al grupo, y tasa de falso rechazo o falso negativo: no se establece la correspondencia entre una persona y su propia plantilla. Frente a las decisiones que afecten jurídicamente a una persona, toda decisión que se adopte en base a ello, como podría ser en sistemas de registro y control horario, la deducción de retribuciones por registro con el sistema, que solo debería efectuarse salvaguardando los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

-Vinculación: un gran número de servicios en línea permiten a los usuarios cargar una imagen para vincularla con el perfil del usuario. El RF puede utilizarse para vincular los perfiles de diferentes servicios en línea (a través de la imagen del perfil), pero también entre el mundo en línea y fuera de línea. No está fuera de lo posible tomar una fotografía de una persona en la calle y determinar su identidad en tiempo real buscando en estas imágenes de perfil público. Servicios de terceros también pueden rastrear fotografías de perfil y otras fotografías públicamente disponibles para crear grandes colecciones de imágenes a fin de asociar una identidad del mundo real con

tales imágenes. Este impacto aumenta con el creciente despliegue de estas tecnologías. Cada individuo puede figurar en uno o varios sistemas biométricos.

-Deben adoptarse medidas de seguridad con motivo del tratamiento de datos biométricos (almacenamiento, transmisión, extracción de características y comparación, etc.) y sobre todo si el responsable del tratamiento transmite esos datos a través de Internet. Las medidas de seguridad podrían incluir, por ejemplo, la codificación de las plantillas y la protección de las claves de codificación aparte del control del acceso y una protección que convierta en virtualmente imposible la reconstrucción de los datos originales a partir de las plantillas. Adicionalmente, uso de máscaras realistas o de uso de fotos para intentar engañar al sistema, siempre en conexión con los avances y el estado de la técnica., teniendo en cuenta que los sistemas biométricos más eficaces a la hora de reconocer a una persona son también los más potencialmente vulnerables

Asimismo, el documento de trabajo sobre biometría, adoptado el 1/08/2003 del GT29, opina que los sistemas biométricos relativos a características físicas que no dejan rastro (por ejemplo la forma de la mano, pero no las huellas digitales) o los sistemas biométricos relativos a características físicas que dejan rastro pero no dependen de la memorización de los datos poseídos por una persona distinta del interesado (en otras palabras, los datos no se memorizan en el dispositivo de control de acceso ni en una base de datos central) crean menos riesgos para la protección de los derechos y libertades fundamentales de las personas (Se pueden distinguir los datos biométricos que se tratan de manera centralizada de los datos de referencia biométricos que se almacenan en un dispositivo móvil y el proceso de conformidad se realiza en la tarjeta y no en el sensor o cuando éste forma parte del dispositivo móvil).

-Se acepta generalmente que el riesgo de reutilización de datos biométricos obtenidos a partir de rastros físicos dejados por personas sin darse cuenta (por ejemplo: huellas digitales) para fines incompatibles es relativamente bajo si los datos no están almacenados en bases de datos centralizadas, sino en poder de la persona y son inaccesibles para terceros. El almacenamiento centralizado de datos biométricos incrementa asimismo el riesgo del uso de datos biométricos como llave para interconectar distintas bases de datos, lo cual podría permitir obtener perfiles detallados de los hábitos de una persona tanto a nivel público como privado. Además, la cuestión de la compatibilidad de los fines nos lleva a la interoperabilidad de diferentes sistemas que utilizan la biometría. La normalización que requiere la interoperabilidad puede dar lugar a una mayor interconexión entre bases de datos.

-Papel del encargado de tratamiento que está obligado a asistir al responsable a la hora de realizar la gestión, y que si desarrolla o suministra un producto como su software, se ha de incorporar al proceso de gestión del riesgo del tratamiento que pretenda realizar el responsable. Opción de auditar las medidas implementadas por el responsable del tratamiento

La reclamada no contempla diversos y variados elementos y escenarios que se han señalado en este apartado en su valoración de riesgos, y ha aportado una evaluación de impacto que fue meramente nominal, por cuanto no ha examinado sus aspectos sustantivos, ni valorado los riesgos ni la proporcionalidad y necesidad de la

implantación del sistema, su afectación a los derechos y libertades de los interesados y sus garantías.

De conformidad con las evidencias de las que se dispone, se considera que los hechos expuestos incumplen lo establecido en el artículo 35 del RGPD.

V

La infracción imputada se tipifica en al artículo 83.4.a) del RGPD que indica:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a)Las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;"

La LOPDGDD establece a efectos de prescripción de la infracción, en su artículo 73.t):

"En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

t) El tratamiento de datos personales sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible."

VI

La determinación de la sanción que procede imponer en el presente caso exige observar las previsiones de los artículos 83.1 y.2 del RGPD, preceptos que, respectivamente, disponen lo siguiente:

"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 9 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias."

"2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate, así como el nú-

mero de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;
b) la intencionalidad o negligencia en la infracción;
c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;
d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;
e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;
f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;
g) las categorías de los datos de carácter personal afectados por la infracción;
h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;
i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;
j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y
k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción."

Dentro de este apartado, la LOPDGDD contempla en su artículo 76, titulado "*Sanciones y medidas correctivas*":

"1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.
f) La afectación a los derechos de los menores.
g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.
h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado.

3. Será posible, complementaria o alternativamente, la adopción, cuando proceda, de las restantes medidas correctivas a las que se refiere el artículo 83.2 del Reglamento (UE) 2016/679."

De acuerdo con los preceptos transcritos, a efectos de fijar el importe de la sanción de multa a imponer en el presente caso por la infracción del artículo 35 del RGPD, de la que se responsabiliza a la entidad reclamada, se estiman concurrentes en calidad de agravantes los siguientes factores que revelan una mayor antijuridicidad y/o culpabilidad en su conducta:

-Artículo 83.2.a) del RGPD: "a*) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido*".

Se trataron datos de un número muy elevado de asistentes, 20.000, sin contemplar el nivel de riesgos alto en relación con la afectación a sus derechos y libertades que puede existir para los tratamientos basados en reconocimiento facial para acceso al Congreso.

- Artículo 83.2.b del RGPD, "*la intencionalidad o negligencia en la infracción*". No se tiene constancia de que la entidad haya obrado dolosamente, aunque la actuación revela una grave falta de diligencia en su conducta en la adopción de medidas proactivas precisas en un régimen tan singular, diferenciado y especial aplicable al tipo de datos que trata, sin que conste que se hayan puesto los medios básicos para que no se produjera. A este respecto, se tiene en cuenta lo declarado en Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006) que, partiendo de que se trata de entidades cuya actividad lleva aparejado en continuo tratamiento de datos, indica que *"…el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto".*

-artículo 76.2.b) de la LOPDGDD "*b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.".* La indiscutible vinculación de la actividad de la reclamada con la realización de tratamientos de datos de carácter personal, al menos de personas físicas asistentes a este tipo de eventos masivos que viene organizando desde hace mucho tiempo (art 76.2.b del RGPD).

En relación con las atenuantes pretendidas por la reclamada:

-Estimando que la infracción no fue continuada, solo duró desde el 22/03/2021 y cesó cuatro semanas después de finalizado el evento, 29/07/2021.

El sistema se usó cada día y durante todo el periodo que duró el Congreso. El número de asistentes diario era presumiblemente de miles de personas, por lo que aunque fuera ese espacio de tiempo, su uso fue intensivo y masivo.

-Sobre la colaboración aportando lo solicitado por la AEPD, se debe indicar que el artículo 5.2 del RGPD en base al principio de responsabilidad proactiva debe ser

interpretado de forma amplia, en el sentido de que el responsable del tratamiento debe no solo demostrar que el tratamiento de datos se ajuste a lo previsto en el mismo, en este caso, antes de implementar datos biométricos, elaborar una EIPD, debiendo asimismo probar que concurren todas las condiciones necesarias para que dicho tratamiento se lleve a efecto. Por tanto, la colaboración y aportación de documentos para acreditar que el tratamiento se ajuste a la normativa es un mínimo exigible, que por ello, no ha de producir atenuante alguna en aso de infracción.

-En relación con la atenuante de que el público asistente estaba familiarizado con las tecnologías y pueden elegir la opción del RF, el procedimiento no se inicia y resuelve por dicho uso, sino por no prever la evaluación de impacto del tratamiento.

Además de lo anterior, añade que los menores en los escasos supuestos que fueron con un asistente, con ellos no se usó el sistema de F. Esta alusión para añadirla como un atenuante en la sanción, no deja de ser puramente secundaria y episódica, cuando nada se ha especificado sobre los menores en el procedimiento, siendo su referencia puramente marginal, y no siendo atendida, siendo además lo se analizaba, la vigencia antes del tratamiento del RF de una EIPD valida.

-Finalmente, el no haber cometido infracciones previas no puede servir como atenuante

Como consecuencia con los elementos que se disponen, se cuantifica la sanción en 200.000 euros.

VII

El artículo 58.2 del RGPD dispone lo siguiente: "*Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:*

[…]"

i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;"

"d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;"

"*La imposición de esta medida es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD*."

El artículo 36.1 y 2 del RGPD establece:

"1*. El responsable consultará a la autoridad de control antes de proceder al*

tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo.

2.Cuando la autoridad de control considere que el tratamiento previsto a que se refiere el apartado 1 podría infringir el presente Reglamento, en particular cuando el responsable no haya identificado o mitigado suficientemente el riesgo, la autoridad de control deberá, en un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado, y podrá utilizar cualquiera de sus poderes mencionados en el artículo 58. Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto. La autoridad de control informará al responsable y, en su caso, al encargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta."

En el presente supuesto, solo se ha valorado la evaluación de impacto exigible antes del tratamiento de los datos del sistema de reconocimiento facial para accesos a MWC de 2021, sin entrar a cuestionar la de 2022.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada,

la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a **GSMA LIMITED**, con NIF ***N4004237F***, por una infracción del artículo 35 del RGPD, de conformidad con el artículo 83.4.a) del RGPD, y a efectos de prescripción, considerada como grave en el artículo 73.t) la LOPDGDD, una multa de 200.000 euros.

SEGUNDO: NOTIFICAR la presente resolución a **GSMA LIMITED** y a **GSMC EVENT PROJECT MANAGEMENT, S.L.**

TERCERO: Advertir al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la ley 39/2015, de 1/10, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), en el plazo de pago voluntario establecido en el art. 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17/12, mediante su ingreso, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº ***IBAN: ES00-0000-0000-0000-0000-0000 (BIC/Código SWIFT: CAIXESBBXXX)***, abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A.. En caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se

encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

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 conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, 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 13/07, 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.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada LPCAP. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-181022

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