¿Cumple la solución para salones de Juego con la normativa existente en materia de protección de datos?

En el desarrollo de la solución, han sido analizadas y puestas en práctica tanto las normativas como las recomendaciones y dictámenes en materia de protección de datos relacionados con el tratamiento de datos biométricos, en particular:

- RGPD Reglamento 2016 679
- LOPD GDD 3/2018
- La protección de datos en las relaciones laborales (AEPD)

Bases jurídicas para la implementación del sistema

Las bases jurídicas sobre las que se sustenta el tratamiento de datos realizado por el sistema de registro de accesos a salones de juego son:

- Normativas que regulan el acceso a este tipo de establecimientos. Dichas normativas, de carácter autonómico, muestran una tendencia a obligar a realizar un estricto control de accesos, creación de fichas de usuarios, verificación de registro de interdicción al juego, etc…

- Consentimiento expreso de los usuarios. El tratamiento de datos de usuarios se realiza bajo el consentimiento expreso y por escrito de los mismos. Los usuarios tienen derecho a métodos alternativos de control de acceso en caso de negar el consentimiento, que son recogidos por la solución. En ningún caso se limita el acceso al establecimiento o a los servicios de los usuarios.

Proceso de desarrollo de solución

El proceso de desarrollo de la solución para salones de juego ha seguido el principio de desarrollo **desde el diseño y por defecto**. Por tanto, los datos recabados han sido minimizados, pseudonimizados, encriptados y se eliminan de manera automática cuando finaliza el objeto del tratamiento o el usuario lo solicita con arreglo a sus derechos ARCO. Además, como empresa especializada en Ciberseguridad, hemos implementado las medidas técnicas y organizativas necesarias para mitigar los riesgos que conlleva un tratamiento de datos de estas características.

Proporcionalidad del sistema

Siguiendo el RGPD y las recomendaciones de la AEPD, el sistema ha sido testeado con respecto al principio de proporcionalidad:

- **Idoneidad**: El sistema biométrico para control de acceso en salones de juego resuelve los requisitos necesarios con el objetivo de cumplir con la normativa;
    - Prohibición de acceso a menores de edad, verificado de manera automática por el lector OCR incorporado
    - Prohibición de acceso a personas en el registro de interdicción al juego, verificado mediante vinculación a las bases de datos existentes por comunidadad.
    - Ahorro de recursos destinados al control de accesos, dado que hasta ahora se realizaban de manera manual por personal del establecimiento.

El sistema opera de manera autónoma, y resuelve el objeto para el que ha sido diseñado.

- **Necesidad**: Hasta ahora, los procesos de control de acceso en salones de juego se realizaban de manera manual. Esto ocasiona problemáticas como:
    - Registros falsos, lo que conlleva que usuarios menores de edad o dados de alta en el registro de interdicción al juego accedieran a los establecimientos.
    - Necesidad de personal de recursos humanos que verifique que los registros son correctos, lo que implica costes para la empresa.
    - Situaciones de conflicto dada la idiosincrasia del sector, en las que en ocasiones el personal del establecimiento no está capacitado para velar por el cumplimiento de la normativa.

- **Proporcionalidad**: La medida no vulnera la vida privada de los usuarios, ya que se siguen los principios básicos en materia de tratamiento de datos personales, y solo persigue una identificación del personal que accede al establecimiento. La no utilización de los datos para fines diferentes al previsto está garantizada gracias a los sistemas de doble encriptación que han sido implementados. Así mismo, existe sistema alternativo de acceso en el que la intervención humana resuelve cualquier inconveniente (posibles falsos rechazos del sistema de reconocimiento facial o errores de sistema) o negativa por parte de los usuarios a ceder sus datos. Además, se ha aplicado en el desarrollo el principio de protección de datos desde el diseño y por defecto para mitigar los posibles riesgos existentes.

Características del sistema con respecto a las recomendaciones RGPD-AEPD

En el desarrollo del sistema han sido tenidas en cuenta las recomendaciones existentes en materia de protección de datos:

- **Minimización de datos**: El sistema utiliza una imagen del cliente para crear una plantilla o vector digital, siendo el único dato personal necesario para el proceso de identificación. Los datos de contacto recabados son los mínimos necesarios para el cumplimiento de la normativa en cada comunidad.
- **Limitación de finalidad**: La finalidad de la tecnología es realizar un control de accesos. Los datos obtenidos no serán tratados ulteriormente y el sistema no está destinado al procesado de otros datos como raza, edad, o emociones del usuario.
- **Periodo de conservación**: Se incorpora un proceso de supresión automatizada de dichos datos en el momento en que el tratamiento deja de tener base jurídica o el cliente solicita su derecho de supresión.
- **Tratamiento de datos en bases de datos reducidas**: Las bases de datos con la que trabaja son reducidas, por lo que el riesgo de uso ilícito es bajo.
- **Tasa de rechazo**: El sistema incorpora un mecanismo de intervención humana con contacto directo al responsable de obra para resolver los posibles errores del sistema (FRR) y ofrecer al usuario un método alternativo en el acceso.

- **Sistema Anti usurpación**: El sistema de identificación incorpora sistema *antispoofing*, por lo que no es posible realizar usurpaciones mediante fotografía.
- **Cifrado de datos**: Se procede a un cifrado de las plantillas biométricas de los usuarios como medida Técnica en caso de uso ilegítimo de los datos obtenidos.
- **Integridad y confidencialidad**: Cibinar, como empresa especializada en Ciberseguridad, aplica diferentes técnicas de codificación, denegación de acceso, y anti extracción al sistema Identity, por lo que los riesgos de uso ilícito de los datos han sido analizados y mitigados sobremanera. Además, Cibinar cuenta con la ISO 27001, (Seguridad de la información) que garantiza la confidencialidad de los datos tratados en los procesos en los que interviene.
- **Transferencia de datos entre empresas**: Cibinar, como empresa de mantenimiento del sistema, tiene acceso a datos de carácter personal, y responde a sus obligaciones legales mediante la formalización de los contratos de tratamiento en función de la naturaleza del servicio, adaptándose a los procesos del cliente

¿Debe realizarse un Estudio de Impacto de protección de datos?

En este sentido, la AEPD pone de manifiesto las diferencias entre los sistemas que se detallan a continuación:

- **Identificación**: La identificación de un sujeto consiste en predecir si éste forma parte de un grupo en un proceso de comparación uno-a-varios (1:n). La ventaja de este sistema radica en que no es necesario portar elementos adicionales (dispositivos, tarjetas RFID, códigos de acceso…) por parte de los usuarios y, por tanto, es el método más efectivo. Estos datos se consideran de categoría especial y para el uso de esta tecnología es necesario realizar previamente un Estudio de Impacto.

.

- **Verificación**: La verificación de un sujeto consiste en la comprobación de que es quien dice ser. Para ello, se realiza un proceso de comparación uno-a-uno (1:1), comparando su vector biométrico con la plantilla almacenada del sujeto. El inconveniente de este procedimiento radica en que el trabajador debe portar un elemento adicional que indique la plantilla con la que deben comparase su vector. Este dato no es considerado dato de categoría especial, por lo que no es necesario desarrollar un Estudio de Impacto.

La solución para salones de Juego está diseñada para realizar un proceso de identificación, por lo que es necesario realizar un Estudio de Impacto.

Recomendaciones al cliente

De manera adicional a las medidas técnicas y organizativas analizadas e implementadas en el sistema, Cibinar recomienda:

- **Informar de forma transparente** a los usuarios del nuevo sistema de control de accesos, sus derechos, los datos tratados (puntos biométricos), su finalidad (control de acceso) y el fin del tratamiento, momento en el cual todo dato almacenado será suprimido de manera automatizada.
- **Solicitar el consentimiento** expreso a los usuarios de forma clara y concisa. El consentimiento será entregado al usuario en el momento de la toma de datos personales.