ANEXO II: INFORMACIÓN COMPLEMENTARIA PARA CLUBES.

¿Está preparado tu club de ajedrez para el nuevo Reglamento General de Protección de Datos?

El 25 de mayo de 2018 entrará en vigor el Reglamento General de Protección de Datos (RGPD) en toda Europa. Pero, ¿qué significa este reglamento y cómo deberían tratarlo los clubs de ajedrez? Compartimos aquí una serie de recomendaciones de interés para los responsables de esta gestión de datos en los clubes de ajedrez.

Por otro lado, si está interesado en disponer de más información sobre el Reglamento General de Protección de Datos puede descargar la Guía del Reglamento General de Protección de Datos para responsables de tratamiento de la Agencia Española de Protección de Datos.

Aspectos legales

El Reglamento General de Protección de Datos impone políticas de confidencialidad, políticas de privacidad y acuerdos de procesador. Con cada tercero (procesadores) que comparta datos personales debe tener un acuerdo. Esto podría ser con formularios impresos, servidores de datos, el sistema con el que está enviando sus boletines, etc. Dentro de ese acuerdo debería haber información sobre la seguridad de los datos, así como la eliminación de los datos cuando los datos ya no son necesarios.

Un punto importante es el derecho al olvido. El club tiene que informar a sus socios de qué manera están recabando datos personales y cómo se pueden eliminar esos datos. La mejor manera de hacerlo es agregarlo a su política de privacidad y poner esa política en el sitio web del club.

Aspectos TIC

El software y los antivirus deben estar siempre actualizados. Las copias de seguridad, que deben protegerse para proteger los datos personales contra pérdida y ransomware, son obligatorias. Todos los soportes de datos (como un USB) deben estar protegidos.

El almacenamiento de datos en la nube no está permitido fuera de la Unión Europea. Si ese es el caso, debe ser cierto que las reglas de protección de datos son las mismas que en la Unión Europea. Por ejemplo, no se permite el almacenamiento de datos en los Estados Unidos ya que no siguen las mismas reglas de protección de datos.

Procedimientos internos

Es importante repasar la organización del club y hacer un inventario de los datos personales que ha captado. Todos los canales y fuentes (correos electrónicos, archivos de Excel, archivos en la nube, archivos impresos, sistema CRM, etc.) deben verificarse y colocarse en un documento con información sobre el tipo de datos personales que posee.

Debe asegurarse de que no todos puedan ver esta información. Tiene que protegerlo con una contraseña o guardarlo en un armario que se puede bloquear. En ese caso, también debe tener una política de claves, quién guarda la llave y quién puede usarla

Importante: solo puede guardar datos personales si tiene un motivo o propósito para ello y siempre con el permiso de esa persona.

Formación

La concienciación es muy importante y debe expresarse claramente a todos los empleados y voluntarios. Asegúrese de que todos sepan qué pueden y qué no pueden hacer y qué procedimientos están en marcha.

El Reglamento General de Protección de Datos (RGPD), aplicable en toda Europa, puede resumirse en los siguientes puntos detallados tema por tema:

Datos personales: Los datos personales consisten en todos los datos que proporcionarán información sobre una persona física identificable. También la información de los miembros de una empresa profesional o los datos personales de los empleados de las organizaciones miembro son parte de esta regulación.

Hay dos tipos de datos personales, los generales (nombre, dirección, código postal, ciudad, provincia, país, lugar de residencia, número de teléfono y/o fax, dirección de correo electrónico, sitio web, sexo, fecha de nacimiento, lugar de nacimiento, títulos, estado civil, perfiles en redes sociales, trabajando para una organización, número de cuenta bancaria, matrícula vehículos) y los específicos (origen étnico, preferencia política, preferencia religiosa, miembro de un sindicato, datos genéticos o biométricos relativos a la identificación, información sobre la salud, orientación sexual, datos penales, información sobre el salario, copia del pasaporte, número de identificación).

El ‘procesamiento’ de datos personales se compone de todas las acciones que realiza con esos datos. Los datos de procesamiento pueden ser una lista de Excel de socios del club, una lista con direcciones para el boletín informativo, etc. Lo más importante que tiene que

hacer con esta información es hacer un inventario de la misma. Haga una descripción clara de los datos que está guardando.

Importante: no se permite el procesamiento de datos personales específicos a menos que tenga un permiso explícito para hacerlo.

Propósito: Es importante que utilice los datos con el mismo propósito que el motivo por el que recibió los datos. La persona en cuestión le dio los datos con un propósito específico (convertirse en socio del club, tramitar su licencia, etc.) y esa es la única razón por la que puede usar esos datos.

Asegúrese de incluir en el acuerdo de incorporación al club que los datos personales serán utilizados de acuerdo con su política de privacidad. Puede agregar la política de privacidad o consultar la política en algún lugar de su sitio web.

Autorización de empleados: Es aconsejable anotar qué personas están autorizadas para ver datos personales y procesar esos datos. Asegúrese de que las personas autorizadas firmen una promesa de confidencialidad.

Permiso de minoría de edad: Si los datos personales pertenecen a una persona menor de dieciséis (16) años, debe contar con la aprobación por escrito (firma en papel) de un padre o tutor legal.

Si ser socio del club depende de la edad, necesita una fecha de nacimiento en el momento de la inscripción. Si no es el caso, no está permitido conservar esos datos personales ya que no los necesita para un propósito específico.

Eliminar datos personales: Los datos personales no pueden mantenerse más tiempo de lo necesario. Entonces, si un socio causa baja del club, los datos personales de esa persona deben ser eliminados.

Acuerdo de procesador: Como organización, no está permitido compartir datos personales sin un acuerdo. Con un acuerdo, solo está permitido compartir datos personales en caso de que sea necesario para lograr un propósito determinado.

Derecho de participación y política de privacidad: El club debe tener una política de privacidad y debe informar a la gente sobre esa política de privacidad en caso de que guarde sus datos personales. Las personas deberían poder encontrar fácilmente esa declaración de privacidad que incluye información sobre sus derechos. La manera más fácil de hacerlo es agregar la política de privacidad en su sitio web y referirse a ella en todos los documentos y correos electrónicos.

Importante hacer y no hacer cuando se trata de privacidad:

- Siempre bloquee su pantalla cuando salga de su escritorio.
- Nunca deje documentos con datos personales en su escritorio o en la impresora.

- Nunca elija guardar sus datos de inicio de sesión automáticamente en su computadora.
- Sepa que las redes públicas no son seguras.
- Presta atención a lo que compartes en las redes sociales.
- Siempre cubra su cámara web para evitar que la gente lo mire a usted.
- Nunca comparta sus datos de inicio de sesión con sus colegas.
- Asegúrate de que tu teléfono móvil esté protegido con una contraseña.

Una persona siempre tiene el derecho de revisar sus datos personales, puede entregarles una copia del formulario de registro.

Seguridad de datos personales: Cuando se trata de la seguridad de los datos personales, debe tomar las siguientes medidas:

- Encripte sus soportes de datos (USB, etc.) y asegúrese de que los datos personales no sean legibles para los demás.
- Cuida la confidencialidad, la integridad y la disponibilidad de los datos personales.
- Cuide la posibilidad de recuperar datos en caso de incidentes físicos / técnicos.
- Pruebe y evalúe la seguridad de forma regular.

Seguridad de acceso: Todos los datos personales deben estar protegidos con una contraseña y si es posible también con un nombre de usuario.

Sistema de seguridad: Para mantener los sistemas lo más seguros posible, debe asegurarse de que se mantengan actualizados. Puede hacerlo activando la instalación automática de las actualizaciones del software. También ponga un buen software antivirus que se actualice automáticamente.

Apoyo: Para proteger los datos de pérdida y ransomware, es necesario realizar una copia de seguridad de forma regular. Asegúrese de que esta copia de seguridad esté almacenada en un lugar seguro.

Documentos seguros: Los datos personales también se almacenan en papel. Todos los documentos con datos personales deben almacenarse en algún lugar de un armario que pueda bloquearse. Solo los empleados que necesitan esa información personal para hacer su trabajo pueden gestionarlos.

En caso de que tenga datos personales en papel y los almacene en algún lugar, es aconsejable establecer una política clave. Escriba en esa política quién conserva la llave y quién puede usar la llave.

Más información en: Agencia Española de Protección de Datos www.agpd.es