GUIA BUENAS PRÁCTICAS MANDOS INTERMEDIOS

IDENTIFICACIÓN Y AUTENTICACIÓN: los empleados con acceso a datos personales, tienen que tener un usuario y contraseña específicos para poder acceder a estos datos.

CONTROL DE ACCESO: los empleados sólo accederán a aquellos datos y recursos que precise para el desarrollo de sus funciones. Los empleados que tengan acceso a datos personales, deberán tener una autorización en la que se especifique si pueden recabar datos, alterarlos y eliminarlos.

REGISTRO DE ACCESOS: cuando un empleado (ej. Un monitor) acceda y tenga que custodiar y trasladar los datos de los clientes y/o empleados, se deberá rellenar una ficha indicando el nombre del monitor, fecha y hora de recogida de la documentación, fecha y hora de la entrega de la documentación y firma del monitor y depositarlos en el lugar que corresponda.

DOCUMENTACIÓN: Toda la documentación que contenga datos personales tiene que estar constantemente custodiada por la persona que esté haciendo uso de la misma. No se puede abandonar el puesto de trabajo dejando la documentación a la vista de cualquier persona y tendrá que ser siempre guardada en un lugar seguro y en caso de que se traten datos especialmente sensibles, se deberá guardar bajo llave.

Hay que guardar toda la documentación que contenga datos personales en carpetas de red, de esta forma se podrán aplicar las medidas de seguridad corporativas (por ejemplo copias de seguridad). Respecto a la información que no se puede almacenar en las carpetas de la red, se debe realizar periódicamente una copia de seguridad (al menos semanalmente).

INICIO NUEVO PROYECTO: Antes de iniciar un nuevo proyecto en el que se vayan a tratar datos personales de empleados, clientes y/proveedores, se tendrá que comunicar y describir el proyecto al buzón de Protección de Datos de Aqualia (protecciondatos@aqualia.es).

Esto es especialmente importante cuando se vaya a contratar un producto y/o servicio (o actualizar dicho contrato) y se vayan a tratar datos personales puesto que se tiene que incluir dentro del contrato de prestación de servicios bien una cláusula de Protección de Datos o bien un Anexo al contrato de prestación de servicios. Esta cláusula de Protección de Datos regulará los derechos y obligaciones de la entidad de Aqualia como responsable del tratamiento con el proveedor como encargado del tratamiento.

Además, si este nuevo proyecto o nueva acción implica el tratamiento de datos, hay que incluirlo en el Registro de Actividades de Tratamiento para posteriormente realizar un análisis de riesgos y en su caso, una evaluación de impacto sobre la privacidad.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO: El nuevo Reglamento Europeo de Protección de Datos elimina la obligación de inscribir los ficheros en la Agencia Española de Protección de Datos pero incluye la nueva obligación de llegar un registro de los tratamientos de los datos que se efectúen en la entidad. Por ello, siempre que se vaya a realizar un nuevo tratamiento de datos, tendrá que incluirse dicho tratamiento en la hoja de "Registro de Actividades de Tratamiento" del Servicio y rellenar los campos que se solicitan en la plataforma "E-Privacy".

PROVEEDORES: si se va a contratar con un proveedor que vaya a tratar datos personales de clientes, empleados y/u otros proveedores del Servicio, este proveedor tendrá que firmar un contrato de encargo de tratamiento de datos personales o incluir una cláusula en el contrato que incluya las obligaciones de protección de datos. Este contrato/cláusula regula las obligaciones y derechos que tiene el proveedor respecto al tratamiento de datos personales de la entidad.

INFORMACIÓN DE PROTECCIÓN DE DATOS: Siempre que se vayan a recabar datos personales por cualquier medio, hay que incluir una cláusula con la información de protección de datos. Esta información se puede mostrar de forma reducida en el documento/formulario donde se recojan los datos personales y luego remitir a una cláusula más extensa donde se explique de forma más detallada el tratamiento de los datos. Antes de recabar los datos personales, por favor, contacta con el Coordinador de Protección de Datos explicando qué datos quieres recabar, de qué colectivo y con qué finalidad quieres tratar sus datos personales para que te proporcione el texto de Protección de Datos ad hoc al tratamiento de datos personales que se vaya a realizar.

CLÁUSULAS DE CONSENTIMIENTO: El nuevo Reglamento Europeo de Protección de Datos exige que cuando se vayan a tratar datos del empleado, cliente y/o proveedor que no tengan relación con la ejecución del contrato, que sea por el cumplimiento de una obligación legal, por protección del interés vital del interesado, para el cumplimiento de una misión realizada en interés público o por interés legítimo, es necesario el consentimiento expreso del cliente, el proveedor persona física o empleado. Por ello hay que tener en cuenta los siguientes puntos:

-Revisa que, en los casos en los que el tratamiento requiera consentimiento los clientes, empleados y/o proveedores han consentido o no consentido el tratamiento de sus datos que se exponen en las hojas donde se recaba el consentimiento. Estas casillas tienen que estar marcadas, ya sea consintiendo o no consintiendo el tratamiento que se solicita, pero siempre tiene que estar marcada una de las dos casillas.

-Cuando vayas a enviar una comunicación comercial, como por ejemplo una newsletter o una oferta comercial, por cualquier medio, comprueba que tienes el consentimiento para enviar esa información comercial. Recuerda que cuando se vaya a enviar una comunicación comercial al correo electrónico de un cliente, tienes que dar la posibilidad de que se pueda dar de baja de ese tipo de comunicaciones.

Si se envía una carta informado al cliente sobre alguna noticia o información que supone una mejora o beneficio, no es necesario el consentimiento, ya que según la AEPD existe interés legítimo por parte de la entidad para realizar dicha comunicación.

-Cuando se vayan a hacer fotografías o videos de los clientes, empleados o el colectivo que corresponda, comprueba que tienes el consentimiento para hacer fotografías y videos y poder utilizarlas para cualquier tipo de publicación o uso que se vaya a hacer sobre las mismas. No se puede utilizar la imagen o voz del cliente o del empleado y utilizarla para publicarla en las redes sociales si no ha consentido previa y expresamente ese cliente o empleado.

- Es necesario llevar un listado actualizado con los consentimientos y revocaciones de consentimientos de las personas, indicando sus datos personales y cuándo nos ha prestado su consentimiento o lo ha revocado y para qué tratamiento lo ha prestado o revocado.

- En cualquier caso, ante la duda es mejor preguntar a Protección de Datos de Aqualia qué podemos hacer o qué no.

TRANSFERENCIAS INTERNACIONALES DE DATOS (TID): Cuando se vaya a llevar un tratamiento de datos personales que supongan una transmisión de los mismos fuera (o el acceso desde) un territorio ubicado fuera de la Unión Europea (UE), se tendrán que cumplir una serie de requisitos. Por ello, siempre que se vaya a realizar una TID, hay que comunicárselo al Coordinador de Protección de Datos.

COMUNICACIÓN ORGANISMOS Y/O AUTORIDAD PÚBLICA: Si e recibe una carta, fax o llamada telefónica por parte de la Agencia Española de Protección de Datos u otra Autoridad de Control de otro país, así como por parte del Cuerpo de Seguridad del Estado, se deberá remitir la misma al Coordinador de Protección de Datos.

En el caso de que se reciba un requerimiento por parte de una entidad pública u autoridad judicial o policial, el cual solicite la entrega de datos personales de clientes, proveedores y/o empleados, es necesario cumplimentar un documento de entrega de datos personales. Puedes solicitarlo al buzón de Protección de Datos de Aqualia.

BRECHAS DE SEGURIDAD: En caso de incidente de seguridad (pérdida, destrucción, alteración accidental o ilícita o robo de cualquier documentación o sistema que contenga datos personales), se deberá seguir las instrucciones detalladas en el documento del "Procedimiento de notificación de violaciones de seguridad". En concreto, tan pronto como se tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales se debe, sin dilación indebida y, de ser posible, a más tardar **24 horas** después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales.

VIDEOVIGILANCIA: A continuación se detallan una serie de puntos de cumplimiento mínimo, que deberán verificarse antes de la instalación y/o una vez instalado, en caso de que no se haya realizado antes:

- No grabar en la vía pública: Las cámaras en ningún momento deberán grabar la vía pública o calle. En caso de ser así, se deberá modificar el campo de grabación de las mismas. La Agencia sólo permite grabar un espacio mínimo (por ejemplo, justo la entrada de la puerta) pero nada más.

- Carteles de información: Tal y como exige la Agencia Española de Protección de Datos “El distintivo se ubicará como mínimo en los accesos a las zonas vigiladas, sean estos exteriores o interiores. Debe tenerse en cuenta que si el lugar vigilado dispone de varios accesos se debe colocar en todos ellos al objeto de que la información sea visible con independencia de por dónde se acceda. (En caso de necesitar el modelo de cartel, por favor, solicítalo al Coordinador de Protección de Datos).
- Impresos: Tener impresos a disposición de las personas que lo soliciten con determinada información adicional sobre el tratamiento de datos. En caso de necesitar el modelo impreso, por favor, solicítalo al Coordinador de Protección de Datos.
- Contrato/cláusula firmada con el Proveedor que realice la instalación y/o el mantenimiento: se deberá firmar antes de cualquier acceso y/o instalación por el Proveedor, un contrato con cláusula de Protección de Datos con la Entidad que vaya a instalar y prestar los servicios de mantenimiento de los sistemas de videovigilancia y custodiarlo debidamente. En caso de necesitar el modelo de contrato de Protección de Datos, por favor, solicítalo al Coordinador de Protección de Datos.
- Medidas de seguridad en los Sistemas de videovigilancia: Se establecerán los requisitos técnicos que exijan usuarios y contraseñas individuales de acceso para cada persona que pueda acceder a las imágenes y que caduquen como máximo al año.
- Derechos de los interesados: Si se recibiera cualquier carta con la solicitud de ejercicio de cualquiera de los derechos o cualquier escrito de la Agencia Española de Protección de Datos, deberá informarse inmediatamente al Coordinador de Protección de Datos.
- Conservación de imágenes: Almacenar las imágenes como máximo un mes. Una vez transcurridos los 30 días, dichas imágenes deberán ser eliminadas.
- Solicitud de imágenes por las Fuerzas y Cuerpos de Seguridad del Estado o autoridades públicas: Si se recibiera cualquier petición por parte de las Fuerzas y Cuerpos de Seguridad del Estado u Organismos públicos, antes de realizar cualquier acción, se deberá informar inmediatamente al Coordinador de Protección de Datos para que especifique cómo proceder.
- Incidencias de seguridad: cualquier incidencia de seguridad que pudiera incurrir, se deberá informar inmediatamente al Coordinador de Protección de Datos.

EVIDENCIAS: Siempre que se traten datos personales, es necesario guardar de forma segura las evidencias, de tal forma que ante cualquier incidente se pueda demostrar el cumplimiento por parte de la entidad.

DERECHOS DE LOS INTERESADOS: Es importante saber identificar el ejercicio de un derecho de protección de datos; por ejemplo, si un cliente solicita que borremos sus datos o quiere conocer qué información tenemos sobre él, está ejercitando un derecho de supresión o de acceso. Si se recibe alguna carta o email de un cliente/candidato/proveedor/empleado en el que se haga referencia a: “datos personales”, “protección de datos”, “derechos de acceso, rectificación, supresión, oposición, limitación, etc” se debe notificar el mismo al Coordinador de Protección de Datos. El ejercicio de estos y otros derechos se gestiona a nivel central, por ello es importante remitir al interesado a la dirección protecciondatos@aqualia.es o a la dirección FOMENTO DE CONSTRUCCIONES Y CONTRATAS, Dpto. Gestión de Clientes y Protección de Datos, Avda. del Camino de Santiago 40, 28050 de Madrid.