VICEPRESIDÈNCIA DEL ORGANISMO AUTÒNOM CONSELL AGRARI MUNICIPAL DE VALÈNCIA

RESOLUCIÓN

Asunto: Instrucción 1/2021 por la que se establecen las funciones y obligaciones del personal del Consell Agrari respecto al tratamiento de datos personales en los sistemas de información del organismo

N.º expedient: 279/2021 **PIAE:** E-70009-2021-000190

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea ('la Carta') y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

La normativa sobre protección de datos de carácter personal ha experimentado una transformación relevante a nivel europeo que se ha visto reflejada con la aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos. Este Reglamento es de aplicación directa en toda la Unión Europea desde el 25 de mayo de 2018 (dos años a partir de la fecha de su entrada en vigor).

Con fecha 5 de diciembre de 2018 se aprobó la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPD y GDD). Esta normativa, que adapta al derecho español el modelo establecido por el Reglamento General de Protección de Datos (RGPD), introduce novedades mediante el desarrollo de materias contenidas en el mismo.

En este sentido, el artículo 32.4 del Reglamento establece que los responsables del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo su autoridad y tenga acceso a datos personales solo puede tratar dichos datos siguiendo las instrucciones del responsable. Lo que nos lleva a realizar una ordenación de las funciones de todo el personal del O.A.M. Consell Agrari Municipal de València —en adelante CAMV— para cumplir con el principio de responsabilidad activa.

El CAMV, con objeto de cumplir con los principios que rigen el desempeño de sus competencias, precisa de un modo constante el tratamiento de datos de carácter personal, correspondientes tanto al personal que trabaja en la propia entidad, como al relativo a los ciudadanos con los que se relaciona y a los cuales presta los servicios que marcan su finalidad.

Estos datos de carácter personal se incorporan y tratan en los diferentes sistemas de información del CAMV, sistemas que pueden ser automatizados o no automatizados. Los primeros están constituidos por el conjunto de aplicaciones informáticas, equipos, redes y soportes en los que se almacenan y tratan los datos de carácter personal, mientras que los segundos se refieren básicamente al tratamiento de estos datos en soporte papel, microfichas, cintas de vídeo, etc., y al conjunto de dispositivos físicos donde se archiva y almacena toda esta información. Su acceso por parte del propio personal nos conduce a establecer unas normas que nos lleven, no sólo a conocer la normativa de protección de datos, sino que además deberemos poder demostrar que hemos tomado las medidas técnicas y organizativas necesarias para garantizar un nivel de seguridad adecuado al riesgo

Atendiendo a estas circunstancias y con el objetivo principal de definir las funciones y obligaciones del personal del CAMV, respecto al tratamiento de los datos de carácter personal incluidos en los sistemas de información municipales, a las previsiones contenidas en el Reglamento General de Protección de Datos, se hace necesario definir sus principales funciones y obligaciones y proceder a difundir la necesidad de garantizar una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas (confidencialidad, integridad, disponibilidad y resiliencia).

****

Primero.- Aprobar la presente Instrucción 1/2021 por la que se establecen las funciones y obligaciones que con carácter general afectan al personal del O. A. M. Consell Agrari Municipal de València respecto al tratamiento de los datos de carácter personal incluidos en los sistemas de información del organismo autónomo municipal, de conformidad con el Reglamento General de Protección de Datos (UE) 2016/679 y con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que se acompaña como Anexo a esta resolución.

Segundo. - La presente instrucción surtirá efectos desde la fecha de su firma.

ANEXO

1. DEBER DE CONFIDENCIALIDAD

Todo el personal empleado público y el personal directivo del O. A. M. Consell Agrari Municipal de València —en adelante CAMV— están obligados a mantener la total confidencialidad de los datos personales tratados o conocidos durante el ejercicio de las funciones y tareas asignadas. Esta obligación se mantendrá aun cuando hubiese finalizado la relación laboral, administrativa o de cualquier otra índole que se tuviera con el CAMV, de conformidad con el artículo 5 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales y de acuerdo con los artículos 52 y 53 del Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.

2. ACCESO, COMUNICACIÓN O CESIÓN A TERCEROS

Con carácter general, la información que contenga datos de carácter personal y que sea utilizada y tratada en el ejercicio de las funciones administrativas encomendadas al personal empleado público, o de la que se tenga conocimiento por razón del cargo o función, no debe comunicarse a terceros no autorizados, salvo que la comunicación sea lícita, según lo establecido en el art. 6.1 del RGPD (UE) 2016/679.

En este sentido, se tendrá muy presente lo establecido con carácter específico en las siguientes leyes:

- Derecho de acceso a la información pública, contemplado en la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la información pública y Buen Gobierno, en concreto la ponderación de intereses prevista en su artículo 15 y en el Reglamento de Gobierno Abierto: Transparencia del Ayuntamiento de Valencia (entrada en vigor el 22 de julio de 2020).
- Derecho de acceso al expediente administrativo previsto en los artículos 28.3, 53.1 a) y b) y 82 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Derechos recogidos en el artículo 4 del Reglamento de Gobierno Abierto: Transparencia del Ayuntamiento de Valencia.
- Artículo 77 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.

Normas de conducta relativas a la transparencia y al acceso a la información

Con el fin de garantizar el principio de transparencia en el desarrollo de sus funciones y responsabilidades, en el ejercicio de su cargo y dentro de su ámbito competencial, el personal empleado público y el personal directivo deben adaptar sus conductas a las siguientes normas:

a) Proporcionar toda la información derivada de las actuaciones, en ejercicio de las funciones y competencias, por los canales de transparencia activa que estén implementados, de acuerdo con la normativa de aplicación.
b) Mantener la confidencialidad y reserva respecto de la información obtenida por razón del cargo, sin perjuicio de las obligaciones derivadas de la normativa de transparencia.
c) No buscar el acceso a información que no les corresponde tener, ni hacer un mal uso de la información de la que toman conocimiento a consecuencia del ejercicio de sus funciones o competencias, así como no facilitar información que saben que es falsa o sobre la que tienen motivos razonables para creer que es falsa.
d) Impulsar el acceso de la ciudadanía a la información municipal como herramienta necesaria del control de la gestión pública derivado del principio de transparencia, garantizando la respuesta ágil y adecuada a las peticiones de acceso.
e) En cualquier caso y cuando se tenga alguna duda respecto a si se puede comunicar o no a terceros información con datos personales se deberá contactar con el responsable del tratamiento quien, en su caso, podrá ponerlo en conocimiento del Delegado de Protección de Datos del CAMV para su análisis y resolución de la cuestión planteada.
f) Solo el personal autorizado podrá enviar datos de carácter personal vía correo electrónico, y resto de medios de comunicación de datos personales, a organismos o entidades externas y con las preceptivas medidas de seguridad que estén establecidas al efecto.

3. INCIDENCIAS

Se entiende por incidencia cualquier evento no esperado que pueda suponer un peligro para la confidencialidad, disponibilidad o integridad de los datos.

Cuando cualquier empleada o empleado público tenga conocimiento o sospecha de cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos de carácter personal tratados en recursos y/o sistemas informáticos del CAMV o contenidos en

documentos y expedientes en papel, se debe informar al responsable del tratamiento, a través de los canales que éste establezca.

Se entiende que estamos ante una incidencia cuando se produzca cualquier evento no esperado que pueda suponer un peligro para la confidencialidad, disponibilidad o integridad de los datos.

A título de ejemplo: accesos o intentos de acceso a equipos aplicaciones o ficheros, automatizados o no, sin contar con la debida autorización; alertas de virus/malware generadas por el antivirus; imposibilidad, por causas diversas, de acceder a un equipo, aplicación o fichero para el que presuntamente se tiene permiso; incidencias relativas a deficiencias en el uso, suministro, reutilización o desechado de soportes; pérdida o extravío de documentos; intentos de hurto o robo en las instalaciones; alteración accidental de datos o registros en las aplicaciones con información crítica; extravío de llaves de locales, oficinas, despachos o armarios que contengan ficheros con datos personales.

4. VIOLACIONES DE SEGURIDAD

Cuando el personal empleado público tenga conocimiento o sospecha de cualquier violación de la seguridad de datos personales que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, se debe informar al CAMV, sin dilación alguna.

La notificación de la violación de seguridad deberá realizarse a la Agencia Española de Protección de Datos por parte del Delegado de Protección de Datos sin dilación y a más tardar 72 horas después de que haya tenido constancia de ella, a través de los canales establecidos al efecto, y con el contenido mínimo que se establece en el artículo 33 del Reglamento General de Protección de Datos, cuando sea probable que constituya un riesgo para los derechos y libertades de las personas.

Si además es probable que la brecha de datos personales entrañe un riesgo alto para los derechos y libertades de las personas físicas, el Consell Agrari Municipal deberá comunicar la brecha a las personas cuyos datos se hayan visto afectados para que puedan tomar sus propias medidas.

5. PUESTO DE TRABAJO

El CAMV suministrará a cada usuario del sistema de información una configuración y software específico para el desempeño de su trabajo. En ningún caso se debe modificar

la configuración inicial de los equipos informáticos (sistema operativo, aplicaciones, conexiones de red, etc.), sin la debida autorización del responsable de seguridad o del administrador de sistemas. En ese supuesto será el personal técnico habilitado al efecto del organismo quien procederá a realizar las actualizaciones correspondientes.

Queda totalmente prohibida la instalación de toda aplicación sin la autorización expresa del responsable designado.

Las conexiones a redes o sistemas exteriores habilitadas por el CAMV no deben emplearse para difundir información de carácter personal a personas no autorizadas.

Se deberá tener habilitada la contraseña de arranque del equipo.

Siempre que el puesto de trabajo quede desatendido, se debe proceder, según el caso, a adoptar las siguientes medidas:

- Bloquear el equipo (pulsando las teclas 'Ctrl-Alt-Supr' y a continuación seleccionar la opción de bloquear el equipo) en el caso de ausencias ocasionales o de corta duración (reuniones, descansos, etc.). Para el desbloqueo posterior se introducirá la contraseña de cada usuario.
- Otro sistema es habilitar el protector de pantalla con contraseña. Se utiliza para que, si nos ausentamos del puesto de trabajo, de manera automática y transcurrido el espacio de tiempo que hayamos indicado en la configuración del protector, se bloquee el equipo, imposibilitando el acceso al mismo a quien desconoce la contraseña para continuar con la sesión.
- Apagar completamente el equipo al término de la jornada diaria de trabajo y en el caso de ausencias prolongadas (vacaciones, permisos, etc.).
- Política de mesas limpias: Consistente en la obligación de guardar la documentación de trabajo al ausentarse del puesto de trabajo y al terminar la jornada laboral. No se debe dejar información sensible a la vista de personas que pudieran hacer un uso indebido de la misma. El cumplimiento de esta política conlleva:

  — Mantener el puesto de trabajo limpio y ordenado

  — Guardar la documentación y los dispositivos extraíbles que no están siendo usados en ese momento, y especialmente al ausentarnos del puesto o al fin de la jornada laboral;

  — No apuntar usuarios ni contraseñas en post-it o similares.

6. ACCESO A RECURSOS Y SISTEMAS MUNICIPALES

Las empleadas y empleados públicos únicamente pueden y deben acceder a la información y a los recursos de los sistemas de información municipales automatizados y no automatizados para los que se esté autorizado, y que resulten imprescindibles para el correcto desempeño de las funciones propias del puesto de trabajo. En este sentido, se debe respetar y cumplir con el nivel de acceso otorgado a cada uno (lectura, modificación, ejecución, impresión, copia, eliminación, etc.), y no podrán acceder y utilizar la información con datos personales para un fin distinto para el que tienen autorización.

Los dispositivos físicos que permiten el acceso a los locales y dependencias municipales donde se encuentran los archivos manuales, los servidores informáticos, etc. (llaves, tarjetas de proximidad, etc.), así como los que permiten el acceso a los equipos informáticos (Smart Card, token, etc.), son personales e intransferibles. En este sentido, y con el fin de minimizar el riesgo de pérdida o extravío de los mismos, se recomienda que se lleven consigo en todo momento.

En los supuestos de cambios de puesto de trabajo de las empleadas y empleados públicos, están obligados a dar de baja todos los accesos a sistemas informáticos que, hayan sido necesarios utilizar por el mencionado personal municipal, por razón de las funciones de dicho puesto de trabajo.

7. CONTRASEÑAS DE ACCESO A SISTEMAS

Las contraseñas que se utilicen por el personal para acceder a los diferentes recursos y sistemas del CAMV para el ejercicio de sus tareas deben mantenerse en secreto, no pueden ser publicadas ni compartidas. A este respecto, se pone de relieve que no se pueden compartir ni facilitar a terceras personas, ya personal empleado público del organismo o colaboradores externos, a fin de garantizar su privacidad y asumir las responsabilidades derivadas de su uso.

No deben anotarse en lugares visibles o fácilmente accesibles (post-it en el monitor del ordenador, debajo del teclado, etc.). Si se tiene conocimiento o indicios de que otra persona distinta de su titular conoce la contraseña, se debe notificar la incidencia de conformidad con lo previsto en el apartado 3 de esta Instrucción y proceder inmediatamente a su cambio.

Las contraseñas elegidas por los usuarios deben ser de estructura compleja (pueden contener letras mayúsculas, minúsculas, números, así como caracteres especiales) y difíciles de deducir (no se debe elegir como contraseña la repetición del usuario, la fecha de nacimiento, la matrícula del vehículo, el nombre de familiares, etc.). Queda

totalmente prohibido usar los mismos identificadores (contraseñas) para acceder a equipos del puesto de trabajo y redes sociales, tanto personales como profesionales.

Las contraseñas de acceso a los sistemas deben cambiarse periódicamente, a pesar de que los propios sistemas, o sus administradores, no notifiquen dicha obligación.

8. DOCUMENTOS EN SOPORTE NO AUTOMATIZADO (PAPEL, CINTAS DE VÍDEO, CINTAS DE IMPRESIÓN Y SOPORTES MAGNÉTICOS, ETC.)

Cuando se proceda a la destrucción de estos documentos, se deben adoptar medidas que eviten el acceso a su contenido o su recuperación posterior. Se recomienda el uso de las destructoras de papel habilitadas a tal fin.

En su traslado, se deben adoptar medidas que eviten la sustracción, pérdida o acceso indebido a su contenido. Los documentos desechados que contengan datos personales no deben utilizarse como ‘material de notas’ ni reutilizable.

La salida de documentos fuera de los locales e instalaciones del Consell Agrari Municipal de València debe ser autorizada por el responsable del tratamiento o por la empleada o el empleado público en quien este delegue y, en todo caso, estar justificada por motivos de trabajo.

Hasta el momento de su devolución al archivo, los expedientes y documentos que se encuentren en fase de revisión o tramitación deben custodiarse de forma que se impida el acceso de personas no autorizadas.

Cada empleada pública o empleado público es responsable de la custodia de la documentación que acumule en su puesto de trabajo.

9. SOPORTES INFORMÁTICOS

En el caso de que se produzcan supuestos justificados por necesidades de trabajo en los que se graben datos de carácter personal en soportes informáticos externos (CD, DVD, dispositivos USB, discos externo,s etc.), estos deben etiquetarse indicando su contenido, así como almacenarse de forma segura.

El contenido de los soportes que vayan a ser retirados, destruidos o reutilizados, debe borrarse previamente, de forma que se impida su recuperación posterior.

Cuando se trasladen, se deben adoptar medidas que eviten la sustracción, pérdida o acceso indebido a su contenido. La salida de soportes fuera de los locales e

instalaciones del organismo, debe ser autorizada por el responsable del tratamiento o por la empleada pública o el empleado público en quien éste delegue y, en todo caso, estar justificada por motivos de trabajo.

10. IMPRESORAS/FOTOCOPIADORAS

Se debe evitar la impresión o fotocopia de documentos que contengan datos de carácter personal en aquellos casos en los que no exista una necesidad real que lo justifique, y en todo caso, con carácter indiscriminado. Los documentos que se impriman y/o fotocopien deben retirarse inmediatamente de la bandeja de salida de las impresoras y fotocopiadoras. En este sentido, los documentos 'olvidados' en dichos dispositivos deberán ser retirados por quien se cerciore de ello.

11. USO DE RECURSOS INFORMÁTICOS

El personal del Consell Agrari Municipal debe proteger y hacer un buen uso de los activos del organismo, en especial los que se utilicen para el tratamiento automatizado o no automatizado de datos personales, evitando en todo momento incurrir en actividades ilícitas o ilegales que infrinjan los derechos del CAMV o de terceros.

Ninguna empleada o empleado debe, bajo ninguna circunstancia, desactivar los sistemas de seguridad de su equipo, incorporar otros, o conectar a los recursos informáticos ningún tipo de equipo de comunicaciones que posibilite la conexión a la red corporativa, sin la oportuna autorización.

Todos los usuarios deben utilizar únicamente software licenciado por el CAMV y homologado para su utilización. En ningún caso se podrán instalar copias ilegales o irregulares de programas, ni borrar ninguno de los programas instalados legalmente. Del mismo modo ninguna persona usuaria debe instalar ni ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, ni dañar o alterar cualquiera de los recursos informáticos.

12. USO DEL MOBILIARIO

Cuando no se utilice la documentación almacenada en las cajoneras, armarios y otros dispositivos análogos, estos deben permanecer debidamente cerrados, al igual que las puertas de los despachos, áreas de trabajo, archivos, etc., siempre que dichas dependencias se encuentren desocupadas o desatendidas.

13. TELETRABAJO

Normas para proteger el dispositivo utilizado en movilidad y el acceso al mismo:

- La persona empleada debe definir y utilizar contraseñas de acceso robustas y diferentes a las utilizadas para acceder a cuentas de correo personales, redes sociales y otro tipo de aplicaciones utilizadas en el ámbito de su vida personal.
- No se debe descargar ni instalar aplicaciones o software que no hayan sido previamente autorizados por la organización.
- Es recomendable evitar la conexión de los dispositivos a la red corporativa desde lugares públicos, así como la conexión a redes WIFI abiertas no seguras.
- Deben mantenerse protegidos los mecanismos de autenticación definidos (certificados, contraseñas, tokens, sistemas de doble factor, …) para validarse ante los sistemas de control de acceso remoto de la organización.
- Si se dispone de un equipo corporativo, no se debe utilizar con fines particulares evitando el acceso a redes sociales, correo electrónico personal, páginas web con reclamos y publicidad impactante, así como otros sitios susceptibles de contener virus o favorecer la ejecución de código dañino.
- Si el equipo utilizado para establecer la conexión remota es personal, debe evitarse simultanear la actividad personal con la profesional y definir perfiles independientes para desarrollar cada tipo de tarea.
- El sistema antivirus instalado en el equipo debe estar operativo y actualizado.
- Siempre ha de verificarse la legitimidad de los correos electrónicos recibidos, comprobando que el dominio electrónico del que procede es válido y conocido, y desconfiando de la descarga de ficheros adjuntos con extensiones inusuales o el establecimiento de conexiones a través de enlaces incluidos en el cuerpo del correo que presenten cualquier patrón fuera de lo normal.
- Si pueden ser gestionadas por la persona empleada, conviene desactivar las conexiones WIFI, bluetooth y similares que no estén siendo utilizadas.
- Una vez concluida la jornada de trabajo en situación de movilidad debe desconectarse la sesión de acceso remoto y apagar o bloquear el acceso al dispositivo.

14. INCUMPLIMIENTO DE LAS FUNCIONES

El incumplimiento de las funciones y obligaciones señaladas en este documento podrá suponer una falta contra las medidas de seguridad de los datos de carácter personal que se tienen que observar en todos los sistemas de información municipales y puede llevar aparejada la aplicación del correspondiente régimen disciplinario.