

**REGLAMENTO DE PROTECCIÓN DE DATOS DEL EXCELENTÍSIMO  
AYUNTAMIENTO DE CARTAGENA**

**EXPOSICIÓN DE MOTIVOS**

Las administraciones, en sus relaciones con la ciudadanía, recopilan gran cantidad de datos personales, necesarios para la adecuada gestión de sus procedimientos y la prestación de un mejor servicio, pero cuya protección resulta obligada en defensa de la privacidad de las personas. Sin embargo, la protección de datos es un derecho muy poco conocido por parte de la propia ciudadanía, a pesar del ingente volumen de memorias, informes preceptivos, sentencias y resoluciones, que desde la Agencia Española de Protección de Datos y el Poder Judicial se han venido emitiendo en los últimos años. Tampoco todas las administraciones son conscientes de que es preciso definir una conducta organizativa donde la protección de datos sea un eje transversal que ligue toda su actuación. Se hace por tanto necesario un análisis de las obligaciones de las mismas en materia de protección de datos y un estudio de la casuística más frecuente y de las colisiones que la aplicación de este derecho puede tener con otros y, con todo ello, establecer un marco normativo, como el que viene dado por el presente Reglamento.

Para la redacción del mismo se han tenido en cuenta las previsiones contenidas en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, posteriormente complementada por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. También se ha tomado en consideración, en lo que procede, el 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 datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), a entrar en vigor el 25 de mayo de 2018. De igual modo, se han explorado los Códigos Tipo de carácter voluntario inscritos en la Agencia Española de Protección de Datos, habiéndose optado, en lo que concierne al presente Reglamento, por realizar una adaptación del Código Tipo para las entidades locales

adheridas a EUDEL (Asociación de Municipios Vascos-Euskadiko Udalen Elkartea), en la medida en que es en absoluto similar al funcionamiento del Ayuntamiento de Cartagena y sus entidades vinculadas o dependientes.

Resultado del mencionado análisis es el presente Reglamento, que se estructura en cuatro capítulos, dos disposiciones adicionales, una disposición transitoria y dos disposiciones finales. El primer Capítulo – Disposiciones generales – determina el objeto y el alcance del presente Reglamento, así como su ámbito de aplicación y el concepto de datos de carácter personal.

El segundo Capítulo – Derechos de los ciudadanos – codifica aquellos derechos que vienen recogidos por Ley y especifica el modo en que deben ser ejercitados en el marco del Ayuntamiento y sus entidades vinculadas o dependientes: acceso, rectificación, cancelación, oposición, impugnación, indemnización y tutela.

De particular importancia resulta el Capítulo III – Obligaciones de la Administración y su personal -, en el que se detallan aquellos aspectos que el Ayuntamiento, sus entidades vinculadas o dependientes y los empleados a su cargo, están obligados a cumplir con respecto a la protección de datos de carácter personal, ya sea en soporte físico o electrónico. Especial mención se hace a la obligatoriedad de disponer de un Documento de Seguridad, en los términos previstos en el artículo 88 del mencionado Real Decreto 1720/2007.

El cuarto Capítulo - Concurrencia del derecho a la protección de datos de carácter personal con otros derechos – contribuye a resolver aquellas cuestiones que puedan plantearse en lo que se refiere a una potencial colisión entre el derecho a la protección de datos de carácter personal y otros derechos de la ciudadanía.

La Disposición Adicional primera prevé un plan anual de formación en la materia para todos los empleados municipales, así como la publicación de un decálogo de protección de datos de carácter personal. La Disposición Adicional Segunda prevé la incorporación de los términos utilizados en el presente Reglamento al Glosario codificado en la "Ordenanza Municipal de Administración Electrónica del Excelentísimo Ayuntamiento de Cartagena".

La Disposición Transitoria Única regula la necesidad de disponer de modelos y formularios normalizados, tanto para el ciudadano, en defensa de sus intereses, como para el Ayuntamiento y sus entidades vinculadas o dependientes, en su funcionamiento cotidiano.

La Disposición Final Primera establece el régimen de modificación y actualización del presente Reglamento, con especial atención a la progresiva adecuación del funcionamiento del Ayuntamiento y sus entidades vinculadas o dependientes al 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 datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), siendo el plazo máximo para tal adecuación el 25 de mayo de 2018. Por último, la Disposición Final Segunda fija el plazo de su entrada en vigor.

## **CAPÍTULO I**

### **Disposiciones generales**

#### **Artículo 1. Objeto.**

El presente Reglamento tiene por objeto regular el tratamiento de los datos de carácter personal que realiza el Ayuntamiento de Cartagena y sus entidades vinculadas o dependientes, así como las sociedades dependientes o vinculadas a éste cuando su capital sea de mayoría pública y ejerzan potestades públicas, a fin de garantizar y proteger las libertades públicas y los derechos fundamentales de los ciudadanos que se relacionan con él y, especialmente, su derecho al honor y a la intimidad personal y familiar, en el marco del respeto a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

#### **Artículo 2. Ámbito de aplicación.**

El presente Reglamento será de aplicación a todo tratamiento de los datos de carácter personal que figuren en ficheros, automatizados o no, del Ayuntamiento y sus entidades vinculadas o dependientes y a toda modalidad de uso posterior de estos datos.

### **Artículo 3. Datos de carácter personal.**

1. Para el desempeño de las competencias que tiene atribuidas, el Ayuntamiento y sus entidades vinculadas o dependientes deben cumplir la normativa de protección de datos de carácter personal al solicitar, recoger, tratar, utilizar o ceder datos de las personas con las que se relaciona. Además, dado que se trata de un derecho fundamental de nueva generación, habrá de poner los medios necesarios para extender la nueva cultura de la protección de datos en sus procedimientos y entre el personal a su servicio.
2. El Ayuntamiento y sus entidades vinculadas o dependientes han de declarar los ficheros en la Agencia Española de Protección de Datos, antes de recabar datos de carácter personal con destino a los mismos, y ha de prestar especial atención al consentimiento de las personas cuando los datos recabados tengan la consideración de especialmente protegidos.

## **CAPÍTULO II**

### **Derechos de los ciudadanos**

#### **Artículo 4. Derecho a la información sobre el uso y finalidad de los ficheros.**

1. Las personas a las que desde el Ayuntamiento y sus entidades vinculadas o dependientes se soliciten datos personales deberán ser previamente informadas de modo expreso, preciso e inequívoco:
  - a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
  - b) Del carácter obligatorio o facultativo de su respuesta a las preguntas o soluciones de información que les sean planteadas.

- c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
  - d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
  - e) De la identidad y dirección de la persona responsable del tratamiento.
2. No será necesaria la información de los apartados b), c) y d) anteriores si se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban. No obstante, se informará siempre a las personas interesadas de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición y del órgano ante el que se podrán ejercitar tales derechos.
  3. La información se proporcionará a través de un medio coherente con el sistema de recogida de los datos; las informaciones y advertencias anteriores deberán figurar claramente en los documentos, formularios, cuestionarios y otros medios, debiéndose procurar que el tipo y tamaño de la letra empleada sea el mismo que el de los demás contenidos de tales medios.
  4. Si las consideraciones de diseño o composición del documento a emplear aconsejasen el recurso a un tipo o tamaño de letra más reducido, se complementará la información a suministrar a través de carteles instalados en un lugar visible y destacado en las oficinas de atención ciudadana, así como de información manifiestamente visible en los portales de internet, en la sede electrónica, en el portal de transparencia, y por cualquier otro medio, de tal modo que pueda ejercitarse el derecho objeto del presente artículo de manera inequívoca.
  5. Cuando los datos de carácter personal no hayan sido recabados de la persona interesada, ésta deberá ser informada de forma expresa, precisa e inequívoca, por el Ayuntamiento y sus entidades vinculadas o dependientes tan pronto como ésta tenga conocimiento del registro de los datos, salvo que ya hubiera

sido informada con anterioridad, del contenido del tratamiento, de la procedencia de los datos, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, y de la identidad y dirección de persona responsable del tratamiento.

6. Con el fin de llevar el derecho de información a su máxima expresión, el Ayuntamiento y sus entidades vinculadas o dependientes informarán de la existencia del presente Reglamento cuando recoja datos personales a través de formularios, indicando su ubicación en la sede electrónica, en el portal de internet del Ayuntamiento y en el portal de transparencia, para su consulta.

#### **Artículo 5. Derecho de acceso.**

1. Los ciudadanos tienen derecho a solicitar y obtener del Ayuntamiento y sus entidades vinculadas o dependientes información de sus datos de carácter personal sometidos a tratamiento, del origen de dichos datos, así como de las comunicaciones realizadas o que se prevé hacer de los mismos.
2. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado en intervalos iguales o superiores a doce meses, salvo que la persona interesada acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo en cualquier momento.

#### **Artículo 6. Derecho de rectificación.**

1. Cuando la persona titular de los datos tuviera constancia de que sus datos personales tratados en un fichero son inexactos, inadecuados, incompletos o excesivos, podrá solicitar y obtener del Ayuntamiento y sus entidades vinculadas o dependientes que los rectifique, corrija o complete.

#### **Artículo 7. Derecho de cancelación.**

1. La persona titular de los datos podrá solicitar y obtener del Ayuntamiento y sus entidades vinculadas o dependientes la cancelación de los mismos cuando:
  - a) Hayan dejado de ser necesarios o pertinentes para la finalidad para la cual fueron recabados.
  - b) Se haya superado el periodo necesario para el cumplimiento de los fines para los que fueron recabados.
2. No obstante, los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre el Ayuntamiento y sus entidades vinculadas o dependientes y la persona interesada.

#### **Artículo 8. Derecho de oposición.**

1. Los ciudadanos tienen derecho a oponerse a un tratamiento de datos por el Ayuntamiento y sus entidades vinculadas o dependientes cuando, sin ser preceptivo el consentimiento previo, existan motivos fundados y legítimos relativos a su concreta situación personal.
2. Las personas interesadas pueden oponerse a un tratamiento de sus datos personales, en cualquier momento, incluso cuando siendo preceptivo el consentimiento previo, lo hubieran prestado con anterioridad.

#### **Artículo 9. Ejercicio de los derechos de acceso, rectificación, cancelación y oposición.**

1. Cualquier petición de acceso, rectificación, cancelación u oposición sobre datos de carácter personal se realizará mediante escrito, físico, únicamente en los supuestos de personas físicas no obligadas de conformidad con el artículo 14.1 de la Ley 39/2015, de 1 de octubre, o electrónico, dirigido a la persona Responsable del Fichero del Ayuntamiento, a través del Registro General o por cualquiera de los medios previstos en la Ley 39/2015, de 1 de octubre de 2015, del Procedimiento Administrativo Común de las Administraciones Públicas.

Cuando la presentación de la petición no se haga de manera presencial la acreditación de la identidad de la persona interesada se realizará de conformidad con lo dispuesto en la Ordenanza de Administración Electrónica del Ayuntamiento de Cartagena.

2. Los derechos de acceso, rectificación, cancelación u oposición de datos son personalísimos y serán ejercidos únicamente por la persona interesada. No obstante, ésta podrá actuar a través de la persona que designe como representante legal cuando se encuentre en situación de incapacidad legal o en minoría de edad que le imposibilite el ejercicio personal de los mismos, en cuyo caso será necesario que la persona que actúe como representante legal acredite tal condición.
3. No se exigirá contraprestación alguna por el ejercicio de los derechos de acceso, rectificación, cancelación u oposición de datos de carácter personal.

#### **Artículo 10. Derecho a la impugnación de valoraciones.**

Las personas interesadas tendrán derecho a impugnar decisiones que les afecten significativamente y que se basen en valoraciones realizadas por el Ayuntamiento o sus entidades vinculadas o dependientes basadas únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad. Esta impugnación se ejercitará como derecho de oposición.

#### **Artículo 11. Derecho a indemnización por daño o lesión en los bienes y derechos de las personas.**

Las personas que, como consecuencia del incumplimiento de lo dispuesto en la normativa de protección de datos por la persona responsable o la encargada del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizadas. Esta responsabilidad se exigirá de conformidad con lo dispuesto en la legislación reguladora del régimen de responsabilidad de las administraciones públicas.



**Artículo 12. Solicitud de tutela ante la Agencia Española de Protección de Datos.**

Cualquier persona interesada a la que se deniegue, total o parcialmente, el ejercicio de los derechos de acceso, rectificación, oposición o cancelación, o entienda que no se le ha facilitado o atendido el ejercicio de su derecho, podrá reclamar ante la Agencia Española de Protección de Datos para que inicie un procedimiento de tutela de sus derechos.

**CAPÍTULO III**

**Obligaciones de la Administración y su personal**

**Artículo 13. Creación, modificación y supresión de ficheros.**

1. La creación, modificación o supresión de ficheros corresponde al órgano competente del Ayuntamiento o a sus entidades vinculadas o dependientes. La resolución o el acuerdo por el que se aprueben los ficheros será objeto de publicación en el Boletín Oficial de la Región de Murcia.
2. Las disposiciones de creación o de modificación de ficheros deberán indicar:
  - a) La identificación y la finalidad del fichero y los usos previstos para el mismo.
  - b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
  - c) El procedimiento de recogida de los datos de carácter personal.
  - d) La estructura básica del fichero.
  - e) La descripción de los tipos de datos de carácter personal incluidos en el mismo.
  - f) Las cesiones de datos de carácter personal.
  - g) Las transferencias de datos que se prevean a países terceros, en su caso.
  - h) El órgano del Ayuntamiento Responsable del Fichero.

- i) El servicio, sección, unidad, órgano o cargo donde se puede ejercitar los derechos de acceso, rectificación, cancelación y oposición.
  - j) Las medidas de seguridad, con indicación del nivel básico, medio o alto exigible.
3. Cuando el Ayuntamiento o sus entidades vinculadas o dependientes tengan dudas importantes respecto a la necesidad de crear un fichero y a la forma de realizarlo, podrán solicitar, con carácter previo a la aprobación de la disposición de carácter general, la emisión de un informe por parte de la Agencia Española de Protección de Datos. A la solicitud acompañará el proyecto de norma que quiere aprobar, en su caso, y una memoria con las dudas cuya aclaración solicita.

#### **Artículo 14. Declaración e inscripción de ficheros.**

Una vez publicada la disposición de creación del fichero en el Boletín Oficial de la Región de Murcia, se notificará a la Agencia Española de Protección de Datos para su inscripción en el Registro de Protección de Datos.

#### **Artículo 15. Propiedad de los datos.**

- 1. El Ayuntamiento y sus entidades vinculadas o dependientes tendrán presente, en todo momento, que los datos personales son propiedad de las personas a las que se refieren y que sólo ellas pueden decidir sobre los mismos. El Ayuntamiento y sus entidades vinculadas o dependientes harán uso de ellos sólo para aquellas finalidades para las que esté facultada debidamente y respetando en todo caso la normativa sobre protección de datos de carácter personal.
- 2. Los datos de carácter personal deberán ser recogidos de forma leal y lícita, por lo que se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

3. Los datos de carácter personal sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas.

**Artículo 16. Calidad en la recogida y el tratamiento de los datos personales.**

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.
2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos, siempre que dicho tratamiento tenga carácter meramente cuantitativo.

**Artículo 17. Mantenimiento y actualización adecuada de los datos personales.**

1. Los datos de carácter personal serán exactos y puestos al día, de forma que respondan con veracidad a la situación actual de la persona afectada. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, inadecuados, incompletos o excesivos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificadas o completados, sin perjuicio de las facultades que a las personas afectadas reconocen el artículo 8 y siguientes de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
2. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados o se haya superado el periodo necesario para el cumplimiento de los fines para los que fueron recabados.

**Artículo 18. Consentimiento de la persona.**

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco de la persona afectada, salvo que la ley disponga otra cosa.
2. El consentimiento podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos. La revocación del consentimiento deberá realizarse necesariamente mediante escrito, físico, únicamente en los supuestos de personas físicas no obligadas de conformidad con el artículo 14.1 de la Ley 39/2015, de 1 de octubre, o electrónico, dirigido a la persona Responsable del Fichero, manifestando tal decisión y ésta deberá responder en el plazo de diez días naturales, contados a partir del día siguiente al de la recepción de la solicitud de revocación del consentimiento, materializando, en su caso, tal revocación dentro del mismo plazo. Si los datos para cuyo tratamiento se revoca el consentimiento hubieran sido comunicados previamente, el Ayuntamiento y sus entidades vinculadas o dependientes deberán notificar la revocación del consentimiento efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último.

**Artículo 19. Recogida de datos especialmente protegidos.**

1. Respecto a los datos personales relativos a la salud, éstos sólo podrán ser recabados y tratados cuando por razones de interés general así lo disponga una ley o cuando la persona interesada consienta expresamente. El personal al servicio del Ayuntamiento y de sus entidades vinculadas o dependientes directamente relacionado con la salud de los trabajadores podrá tratar los datos de carácter personal relativos a la salud de las personas que atiendan, de acuerdo con lo dispuesto en la normativa vigente en materia de sanidad y de protección de la salud y prevención de riesgos laborales.
2. El tratamiento de datos relativos a ideología, religión, creencias y afiliación sindical, requiere el consentimiento expreso y por escrito de la persona interesada. Los datos de carácter personal que se refieran a la vida sexual, salud u origen racial de las personas sólo serán recabados, tratados y cedidos cuando por razones de interés público así lo establezca una ley o la persona interesada consienta expresamente. En el caso en que se recaben datos

relativos a la ideología, la religión o las creencias de la persona interesada, ésta será advertida de su derecho a no consentir el tratamiento de tales datos.

**Artículo 20. Facilitación a las personas del ejercicio de sus derechos.**

1. El Ayuntamiento y sus entidades vinculadas o dependientes no sólo permitirán, sino que facilitarán a las personas el ejercicio de los derechos enumerados en el presente Reglamento. A este efecto creará los procedimientos administrativos oportunos para que se puedan ejercer fácilmente los derechos de acceso, rectificación, cancelación y oposición.
2. Así, el Ayuntamiento y sus entidades vinculadas o dependientes quedan obligados mediante el presente Reglamento a:
  - a) Arbitrar un procedimiento específico para facilitar el ejercicio de estos derechos.
  - b) Poner a disposición de la ciudadanía modelos para el ejercicio de sus derechos de acceso, rectificación, cancelación y oposición, que estarán a disposición de las personas interesadas en el Registro General, en las oficinas de asistencia en materia de registro, en la sede electrónica del Ayuntamiento, en las subsedes, si procede, en los portales municipales de internet y en el portal de transparencia.
  - c) Informar y formar adecuadamente al personal que tenga acceso a los datos del fichero para que puedan atender adecuadamente a la ciudadanía en el ejercicio de sus derechos.
  - d) Incorporar progresivamente en las nuevas aplicaciones informáticas las funcionalidades que faciliten el ejercicio de los derechos de acceso, rectificación, cancelación u oposición, con el objeto de permitir a las personas interesadas la identificación de los procedimientos para el ejercicio de sus derechos.

**Artículo 21. Contratación para la prestación de servicios que conlleven acceder a datos personales.**

1. Cuando el Ayuntamiento y sus entidades vinculadas o dependientes faciliten el acceso a datos personales a una tercera persona o entidad para que realice un tratamiento concreto con ellos por encargo de la propia administración, no se considerará comunicación de datos.
2. Independientemente del coste de la prestación del servicio, el Ayuntamiento y sus entidades vinculadas o dependientes regularán la realización del tratamiento con la parte prestataria, mediante contrato por escrito en formato electrónico, cláusula administrativa particular en el mismo formato, o en cualquier otra forma, siempre que permita acreditar su celebración y contenido.
3. En el documento vinculante entre el Ayuntamiento o sus entidades vinculadas o dependientes y una tercera persona o entidad, quedarán expresamente recogidas las siguientes obligaciones para la empresa o entidad prestataria:
  - a) Asumir la obligación genérica de cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y, expresamente, en lo indicado en su artículos 9 y 10, y en el Reglamento de desarrollo de la citada Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, comprometiéndose explícitamente a informar y formar a su personal en las obligaciones que de tales normas dimanen.
  - b) Utilizar la información y datos de carácter personal que se le faciliten única y exclusivamente para la finalidad de realización de las actividades contempladas en el contrato de cesión de datos.
  - c) Tratar la información conforme a las instrucciones que consten o que se trasladen posteriormente.

- d) Guardar el secreto profesional, tanto la empresa como el personal a su cargo, sobre todas las informaciones, documentos y asuntos a los que tenga acceso o conocimiento durante la vigencia del contrato, estando obligados a no hacer públicos o enajenar cuantos datos conozcan como consecuencia o con ocasión de su ejecución, incluso después de finalizar el plazo contractual.
- e) Cumplir las medidas de seguridad y adoptar las medidas necesarias de índole técnica y organizativa que garanticen la seguridad de los datos personales que se le faciliten, conforme al nivel de seguridad del fichero de que se trate, de tal manera que eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o de medio físico o natural.
- f) No reproducir, ni comunicar, ni ceder a terceras personas o entidades información a la que tengan acceso durante la ejecución del contrato.
- g) Poseer un Documento de Seguridad formalizado y documentado, en el que se determinen las medidas de índole técnica y organizativa que deben implantarse atendiendo a la naturaleza de los datos. A tal fin, la parte adjudicataria deberá aportar con anterioridad a que se produzca la cesión de datos, en su caso, una memoria descriptiva de las medidas que adoptará para asegurar la confidencialidad e integridad de los datos manejados y de la documentación facilitada, con indicación asimismo del nombre de la persona Responsable de la Seguridad en su empresa o entidad de esos datos y tratamientos, con especificación de su perfil profesional.
- h) Informar al Ayuntamiento o a sus entidades vinculadas o dependientes, de modo inmediato, sobre cualquier sospecha relacionada con fallos o fugas del sistema de seguridad y protección de la información que pudiera ser detectado durante la ejecución del contrato.
- i) Facilitar, en su caso, el control y auditoría por parte del Ayuntamiento o sus entidades vinculadas, mediante la aportación de la información que se le

solicite e incluso, excepcionalmente, el acceso a los locales que se determinen. Incluso autorizar al Ayuntamiento y a sus entidades vinculadas o dependientes la posibilidad de utilizar registros de control en los ficheros facilitados.

- j) No subcontratar la actividad, en todo o en parte, sin autorización expresa para ello. En este supuesto deberán recogerse por escrito en formato electrónico los datos que podrán facilitarse por la empresa adjudicataria a la empresa subcontratista y todas las obligaciones de ésta última, que serán como mínimo las de aquella, respecto del Ayuntamiento y sus entidades vinculadas o dependientes.
  - k) Borrar los datos o devolver el soporte informático en el que constan los datos personales que provienen de los ficheros que se le han facilitado, una vez prestados los servicios requeridos, sin conservar copia alguna del mismo, ni siquiera de seguridad, y sin que ninguna persona externa, física o jurídica, entre en conocimiento de los datos. Asimismo devolverá o destruirá todos los soportes magnéticos, soportes ópticos o cualquier otro tipo de soporte procesable, estando en cualquier caso a lo dispuesto en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, en lo que concierne al borrado de información.
4. Con la finalidad de asegurar el cumplimiento de las prescripciones contempladas en el presente artículo, en los pliegos de cláusulas administrativas generales o de condiciones técnicas, se recogerán las anteriores obligaciones para que sean asumidas por las personas participantes en los procedimientos de contratación administrativa.
5. Será necesario recoger en el contrato escrito que suscriban ambas partes, al menos, las cláusulas referidas a:
- a) Acceso a locales donde se tratan datos personales.



- b) Deber de confidencialidad de las personas que accedan a datos de carácter personal.
- c) Cumplimiento de medidas de seguridad por parte de esas mismas personas.

**Artículo 22. Tipos de fichero y niveles de seguridad.**

1. De conformidad con lo dispuesto en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.
2. Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, los relativos a la administración tributaria, los de las mutuas de accidentes de trabajo y aquellos que permitan evaluar la personalidad deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.
3. Los ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas y los que contengan datos derivados de actos de violencia de género deberán reunir, además de las medidas de nivel básico y medio, las calificadas de nivel alto.

**Artículo 23. Funciones y obligaciones de las personas que tratan datos de carácter personal.**

1. Todo el personal al servicio del Ayuntamiento o sus entidades vinculadas o dependientes que realice tratamientos de datos de carácter personal, de forma general o excepcional, deberá respetar la legislación y normativa aplicable al respecto, para lo que deberán aplicar de manera diligente lo establecido en la mencionada normativa y en el presente Reglamento.

2. Quienes tengan personas bajo su responsabilidad deberán formarlas debidamente en sus deberes y obligaciones respecto al tratamiento y protección de datos de carácter personal, prestando especial atención a la formación en la fase de acogida, cuando se incorporen por primera vez a sus equipos.
3. En el ámbito del Ayuntamiento y sus entidades vinculadas o dependientes, se identifican las siguientes figuras, como potenciales agentes en la protección de datos de carácter personal:
  - a) La Alcaldía, o en su caso, quien tenga delegadas las competencias en materia de Protección de Datos del Ayuntamiento de Cartagena, asumirá la máxima responsabilidad de la efectiva aplicación de la legislación y normativa.
  - b) El Responsable del Fichero: el Ayuntamiento se constituye como responsable último de todos los ficheros que contengan datos de carácter personal en sus instalaciones. Asimismo, le corresponde decidir sobre la finalidad, contenido y uso del tratamiento de datos de carácter personal. Para la realización de tareas operativas relacionadas con la seguridad de los ficheros la Alcaldía, o en su caso, quien tenga delegadas las competencias en materia de Protección de Datos del Ayuntamiento de Cartagena, designará, en caso de que delegue en otra, a la persona física que, de entre su personal, deba realizar las tareas de control de uno o varios ficheros, sin que dicha delegación de actividades suponga una exoneración de las responsabilidades que, en materia de seguridad de datos de carácter personal, corresponde al Ayuntamiento.
  - c) Responsable de Seguridad: la persona encargada de definir y velar por el cumplimiento de la estrategia global en materia de seguridad de la información en la administración y de la correcta adecuación de la misma a lo establecido en la legislación y normativa relativa a la protección de datos de carácter personal. Tiene atribuidas por la persona Responsable del Fichero la función de coordinar y controlar las medidas de seguridad aplicables. En el ejercicio de sus competencias podrá recabar la colaboración de Letrado Consistorial, Técnico de Administración General o Técnico en Administración

Electrónica, pertenecientes al Grupo de Proyecto para la implantación de la Administración Electrónica, según Ordenanza Municipal de Administración Electrónica, a fin de asegurar la idoneidad de las propuestas o acciones que se deban realizar, en el ámbito jurídico.

- d) Persona o entidad Encargada del tratamiento: la persona física o jurídica que, sola o conjuntamente con otros, trate datos personales por cuenta del Ayuntamiento y sus entidades vinculadas o dependientes. Cabe la posibilidad de que el Ayuntamiento o sus entidades vinculadas o dependientes contraten los servicios necesarios para llevar a cabo tratamientos de la información.
- e) Persona colaboradora o coordinadora en materia de protección de datos: la persona que puede designar el Ayuntamiento con el encargo de coordinar, dinamizar y extender la nueva cultura de la protección de datos. Podrá coincidir o no con alguna de las figuras anteriores.

#### **Artículo 24. Documento de Seguridad.**

- 1. El Ayuntamiento implantará la normativa de seguridad mediante un Documento de seguridad de obligado cumplimiento para el personal con acceso a los datos de carácter personal y a los sistemas de información, tanto de sus órganos como de sus entidades vinculadas o dependientes.
- 2. El Documento deberá contener, como mínimo, los siguientes aspectos:
  - a) Ámbito de aplicación del Documento, con especificación detallada de los recursos protegidos.
  - b) Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en la normativa vigente y en el presente Reglamento.
  - c) Funciones y obligaciones del personal.

- d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
  - e) Naturaleza de los datos sujetos a protección.
  - f) Procedimiento de notificación, gestión y respuesta ante las incidencias.
  - g) Procedimientos de realización de copias de respaldo y de recuperación de los datos.
  - h) Controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio Documento de Seguridad.
  - i) Medidas a adoptar cuando un soporte o documento tenga que ser transportado, desechado o reutilizado.
3. El Documento deberá mantenerse actualizado en todo momento y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.
  4. El contenido del Documento deberá adecuarse en todo momento a las disposiciones vigentes en materia de seguridad de los datos de carácter personal y ser coherente con la Política de Seguridad de la Información del Ayuntamiento.

**Artículo 25. Comunicación de sus obligaciones a las personas con acceso a datos.**

1. Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas.
2. La persona Responsable del Fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

#### **Artículo 26. Sistemas de identificación y autenticación.**

1. La persona Responsable del Fichero se encargará de que exista una relación actualizada de personas que tengan acceso autorizado a los sistemas de información y de establecer procedimientos de identificación y autenticación para dicho acceso.
2. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.
3. Las contraseñas se cambiarán con la periodicidad que se determine en el Documento de Seguridad y mientras estén vigentes se almacenarán de forma ininteligible.
4. Se establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de toda persona usuaria que intente acceder a los sistemas de información y la verificación de que está autorizada para tal fin.
5. Las personas usuarias serán siempre personas físicas, identificadas de manera única, no permitiéndose los accesos de personas usuarias mediante cuentas o identificadores compartidos. Cada persona usuaria será responsable de todas las actuaciones que se realicen con su identificador.
6. Se limitará a tres veces la posibilidad de intentar reiteradamente el acceso no autorizado a los sistemas de información, bloqueándose los mismos tras estos tres intentos, de tal manera que el usuario tenga que contactar con el administrador del sistema para su desbloqueo, si procede.

#### **Artículo 27. Control de acceso a aplicaciones informáticas.**

1. Las personas usuarias tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones. Se establecerán mecanismos para evitar que una persona usuaria pueda acceder a datos o recursos con derechos distintos de los autorizados.

2. La relación de personas usuarias, a la que se refiere el artículo anterior del presente Reglamento, contendrá el acceso autorizado para cada una de ellas. Exclusivamente el personal autorizado para ello en el Documento de Seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos en el Documento de Seguridad.

**Artículo 28. Registro de accesos en ficheros de nivel alto.**

1. De cada acceso se guardarán, como mínimo, la identificación de persona usuaria, la fecha y hora en que se realizó, el fichero al que se ha accedido, el tipo de acceso y si ha sido autorizado o denegado.
2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro al que se ha accedido.
3. Los mecanismos que permiten el registro de los datos detallados en los apartados anteriores estarán bajo el control directo de la persona Responsable de Seguridad, sin que se deba permitir, en ningún caso, la desactivación ni la manipulación de los mismos.
4. El período mínimo de conservación de los datos registrados será de dos años.
5. La persona Responsable de Seguridad se encargará de revisar periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y de los problemas detectados, al menos una vez al mes.

**Artículo 29. Acceso a locales donde estén ubicados los equipos con la información.**

1. Solamente el personal autorizado en el Documento de Seguridad podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.
2. Los locales donde estén ubicados los sistemas de información de nivel alto deberán estar dotados de un sistema de control de accesos que permita el

acceso sólo a las personas autorizadas, disponiendo en todo momento de un registro de las personas y accesos realizados.

### **Artículo 30. Acceso a datos a través de la red.**

La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni sea manipulada por terceras personas. Los datos sólo se mantendrán cifrados durante el proceso de transmisión.

### **Artículo 31. Régimen de trabajo en estaciones de trabajo, portátiles y en modalidad Cloud.**

1. La ejecución de tratamientos de datos de carácter personal fuera de los sistemas informáticos del Ayuntamiento o de sus entidades vinculadas o dependientes, desde estaciones de trabajo o equipos portátiles particulares o propiedad de aquél o aquéllas, deberá ser autorizada expresamente por la persona Responsable del Fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado y su cifrado.
2. En los casos en los que se haga uso de computación en Cloud, en cualquiera de sus modalidades, se estará a lo dispuesto en la Ordenanza de Administración Electrónica del Excelentísimo Ayuntamiento de Cartagena.

### **Artículo 32. Gestión de soportes.**

1. Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen sólo a aquellos usuarios con acceso autorizado y deberán ser inventariados y etiquetarse para almacenarse en un lugar con acceso restringido al personal autorizado para ello en el Documento de Seguridad.

2. La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada por la persona Responsable del Fichero.
3. Deberá establecerse un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, la persona emisora, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.
4. Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario, adoptando para ello las medidas previstas en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
5. Cuando los soportes se vayan a distribuir o vayan a salir fuera de los locales en que se encuentren ubicados los ficheros, como consecuencia de operaciones de mantenimiento, salvaguarda o de necesidades de trabajo, se adoptarán las medidas pertinentes encaminadas a evitar cualquier manipulación indebida de la información almacenada.

### **Artículo 33. Copias de respaldo y recuperación de los datos.**

1. La persona Responsable del Fichero o, por delegación, la persona Responsable de Seguridad, se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.
2. Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberán garantizar su reconstrucción en el estado en que se encontraban en el momento de producirse la pérdida o destrucción.



3. Deberán realizarse copias de respaldo de los ficheros con carácter diario, salvo que en dicho lapso no se hubiera producido ninguna actualización de los datos.
4. Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, cumpliendo en todo caso las medidas de seguridad exigidas en el presente Reglamento.

**Artículo 34. Ficheros temporales, copias de trabajo de documentos y pruebas con datos reales.**

1. Los ficheros temporales o copias de documentos que se hubieran creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda, con arreglo a la naturaleza de la información y, en su caso, de las finalidades de los mismos, en relación con la mayor o menor necesidad de garantizar la confidencialidad, integridad y disponibilidad de la información.
2. Todo fichero temporal o copia de trabajo así creado será borrado una vez que haya dejado de ser necesario para los fines que motivaron su creación.
3. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

**Artículo 35. Registro de incidencias.**

1. El procedimiento de notificación y gestión de incidencias contendrá necesariamente un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma.
2. Se deberán consignar en este registro los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los

datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

3. Será necesaria la autorización por escrito de la persona Responsable del Fichero para la ejecución de los procedimientos de recuperación de los datos.

#### **Artículo 36. Circuito de datos en soporte papel y destrucción de copias.**

1. Se evitará el uso de listados o copias impresas en papel que contengan datos personales. Cuando resulte imprescindible, se establecerá un sistema para que sólo las personas usuarias autorizadas tengan acceso a su contenido y evitar que la información sea accesible por personas no autorizadas.
2. En el supuesto de que sea necesario que la información en papel mencionada en el apartado anterior salga fuera de los locales administrativos se adoptarán las medidas necesarias para evitar un uso indebido de la misma.
3. Cuando los listados o copias impresas en papel dejen de ser necesarias se adoptarán las medidas necesarias para su destrucción.

#### **Artículo 37. Auditorías.**

1. Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa anual, o en el supuesto de que se produzca un ciberincidente en los términos previstos en el "Reglamento de Evidencias Digitales del Excelentísimo Ayuntamiento de Cartagena", que verifique el cumplimiento del presente Reglamento y de los procedimientos e instrucciones vigentes en materia de seguridad de datos.
2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente Reglamento y a la normativa vigente relativa a protección de datos de carácter personal, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá,

igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

3. Los informes de auditoría serán analizados, en su caso, por la persona Responsable de Seguridad, quien comunicará las conclusiones al Responsable del Fichero para que se adopten las medidas correctoras adecuadas. Los informes de auditoría realizados quedarán a disposición de la Agencia Española de Protección de Datos.

### **Artículo 38. Actuaciones con respecto a ficheros no automatizados.**

1. En lo que concierne a las actuaciones con respecto a los ficheros no automatizados, los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Igualmente se deberá identificar el tipo de información que contienen, ser inventariados y almacenarse en lugares controlados por el personal autorizado para ello en el Documento de Seguridad.
2. La persona Responsable del Fichero, de manera coordinada con el Jefe de Archivo, deberá establecer los procedimientos que deban seguirse en el archivo de los ficheros no automatizados. Dichos procedimientos estarán dirigidos a garantizar la correcta conservación de los documentos, la localización y consulta de la información y a posibilitar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.
3. Mientras la información no se encuentre en el Archivo Municipal, por estar en revisión o tramitación, la persona que se encuentre a cargo de ella deberá custodiarla e impedir el acceso a la misma de personas no autorizadas.
4. Existirá para estos ficheros una persona Responsable de Seguridad con las mismas responsabilidades y funciones que para los ficheros automatizados.
5. Estos ficheros se someterán a una auditoria interna o externa al menos cada dos años.

6. El acceso a la documentación se limitará al personal autorizado en el Documento de Seguridad. Cuando existan múltiples personas, deberán establecerse mecanismos que permitan identificar los accesos.
7. El local en que se encuentre el fichero deberá estar dotado de puertas con llave o dispositivo equivalente, debiendo estar cerradas cuando no sea preciso el acceso a los documentos. Si ello no fuera posible, la persona Responsable de Seguridad hará un informe motivado proponiendo alternativas. En cualquier caso, los armarios, archivadores o elementos de almacenamiento deben tener sistemas que obstaculicen el acceso no autorizado.
8. La copia de documentos sólo podrá ser realizada por personal autorizado. Cuando se destruyan las copias, se hará mediante procedimientos que impidan su posterior recuperación.
9. En el traslado de estos ficheros deberán adoptarse medidas de seguridad que impidan el acceso a la documentación de personas no autorizadas, o la manipulación de la información o la detección de accesos no autorizados.

### **Artículo 39. Deber de secreto profesional.**

1. Toda persona que intervenga en cualquier fase del tratamiento de los datos de carácter personal de ficheros está obligada al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar su relación de servicio con el Ayuntamiento o sus entidades vinculadas o dependientes.
2. El incumplimiento del deber de secreto será sancionado de conformidad con lo previsto en la legislación vigente y traerá consigo, en su caso, las responsabilidades penales, disciplinarias y ante terceras personas o entidades que la misma establece.

3. Todas las personas al servicio del Ayuntamiento y de sus entidades vinculadas o dependientes están obligadas a guardar el secreto profesional en cuanto a los datos de carácter personal a los que tengan acceso.

**Artículo 40. Obligaciones en las comunicaciones de datos.**

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a una tercera persona para el cumplimiento de fines directamente relacionados con las funciones legítimas del Ayuntamiento y de sus entidades vinculadas o dependientes y de la parte cesionaria, con el consentimiento expreso del interesado.
2. El consentimiento exigido en el apartado anterior no será preciso:
  - a) Cuando la cesión esté autorizada en una ley.
  - b) Cuando se trate de datos recogidos de fuentes accesibles al público.
  - c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceras personas o entidades. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
  - d) Cuando la cesión se produzca entre el Ayuntamiento y sus entidades vinculadas o dependientes y otras administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos, con finalidades cuantitativas.
  - e) Cuando los datos hayan sido recogidos o elaborados por el Ayuntamiento o sus entidades vinculadas o dependientes con destino a otra administración, o cuando se realice para el ejercicio de competencias sobre las mismas materias.
  - f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia, que requiera acceder a un fichero, o

para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a una tercera persona, cuando la información que se facilite a la persona interesada no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.
4. El consentimiento para la comunicación de los datos de carácter personal tiene carácter revocable.
5. Aquella persona a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones legales y normativas objeto del presente Reglamento.
6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

**Artículo 41. Procedimiento para las cesiones de datos que requieran el consentimiento de la persona interesada.**

En el caso de cesiones de datos al Ayuntamiento o a sus entidades vinculadas o dependientes que precisen del consentimiento de la persona interesada, se procederá de la siguiente forma:

- a) El órgano solicitante remitirá su petición a la persona Responsable del Fichero, que valorará la oportunidad de la cesión así como su legalidad, sin perjuicio de que pueda recabar el asesoramiento jurídico de quien tenga atribuida dicha función en el Ayuntamiento.

- b) La persona Responsable del Fichero remitirá la carta de condiciones, en formato electrónico, al órgano solicitante para que la firme mediante recibí y conforme.
- c) La persona Responsable del Fichero comprobará la autorización prestada por las personas afectadas, debiendo solicitarles expresamente su consentimiento si fuera necesario, y llevará a cabo un sistema de marcado en las fichas personales generadas al efecto, donde consten en cada momento las cesiones realizadas, a fin de garantizar el efectivo ejercicio de los derechos de acceso, rectificación y cancelación de las personas interesadas.
- d) La persona Responsable del Fichero comunicará los datos a la parte cesionaria en formato electrónico. Las cesiones realizadas serán reflejadas en el correspondiente registro electrónico de entradas y salidas del Documento de Seguridad del fichero.

**Artículo 42. Procedimiento para las cesiones de datos que no requieran el consentimiento de la persona interesada.**

En el caso de cesiones de datos que no precisen del consentimiento de la persona interesada, tales cesiones se llevarán a cabo mediante la supervisión de la persona Responsable del Fichero. Sin carácter exhaustivo, se consideran cesiones de este tipo:

- a) La cesión realizada a organismos judiciales y administrativos, de conformidad con las diferentes leyes aplicables, en el ejercicio de las funciones que tienen atribuidas y en los supuestos y condiciones establecidos en las citadas normas.
- b) La cesión de datos personales pertenecientes a empleados del Ayuntamiento y de sus entidades vinculadas o dependientes realizada a quienes ostenten su representación sindical, en cumplimiento de la legislación sobre libertad sindical vigente en cada momento.
- c) La cesión de datos de carácter personal relativos a la salud, si es necesaria para solucionar una urgencia que requiera acceder a un fichero automatizado, o

para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad y prevención de riesgos laborales vigente en cada momento.

- d) La cesión que se efectúa previo procedimiento de disociación, es decir, de modo que la información que se obtenga no pueda asociarse a persona determinada o determinable.

**Artículo 43. Utilización y tratamiento de datos del Padrón Municipal de Habitantes.**

1. Las finalidades para las que se pueden utilizar los datos del Padrón Municipal de Habitantes son las establecidas al efecto en la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local:
  - a) Determinar la población del municipio.
  - b) Constituir prueba de la residencia en el municipio y del domicilio habitual en el mismo.
  - c) Elaborar estadísticas sobre composición de familias, características económicas, nivel educativo, matrimonio, fecundidad y defunciones.
2. Los datos del Padrón Municipal de Habitantes se cederán a otras administraciones públicas que lo soliciten, sin consentimiento previo de la persona afectada, cuando les sean necesarios para el ejercicio de sus competencias, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes, en los términos previstos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
3. Los requisitos para la cesión de datos entre órganos del Ayuntamiento y con sus entidades vinculadas o dependientes son los mismos que los previstos para la cesión entre administraciones públicas. En consecuencia, cuando la cesión de datos del Padrón Municipal de Habitantes sea para el ejercicio de una



competencia que corresponde al propio Ayuntamiento o a sus entidades vinculadas o dependientes, en la que el domicilio sea dato relevante, se comunicarán los mismos sin consentimiento de la persona interesada. Cuando concurra dicha circunstancia habrá de entenderse que existe compatibilidad de fines.

4. No ocurrirá lo mismo cuando los datos se cedan desde otros ficheros que no sean el del Padrón Municipal de Habitantes. En consecuencia, no podrá admitirse el uso compartido de los datos de un fichero en el que se recojan datos de carácter personal para la tramitación de un expediente administrativo, ni incluso a otro órgano del Ayuntamiento y a sus entidades vinculadas o dependientes, para el desarrollo de una competencia de ésta que no se encuentre expresamente contemplada entre las finalidades del fichero afectado, salvo que una Ley disponga otra cosa.

## **CAPÍTULO IV**

### **Concurrencia del derecho a la protección de datos de carácter personal con otros derechos**

#### **Artículo 44. El derecho de acceso a la información.**

El derecho a obtener información del Ayuntamiento o de sus entidades vinculadas o dependientes corresponde a toda persona por su condición de ciudadana, en los términos previstos en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, codificados en la Ordenanza de Administración Electrónica del Excelentísimo Ayuntamiento de Cartagena.

#### **Artículo 45. Publicidad y difusión de los actos administrativos.**

1. Con carácter general, cuando deba procederse a la publicación o difusión por cualquier medio de los actos administrativos que deban darse a conocer a las personas interesadas o al público en general, y la información a suministrar contenga datos de filiación de personas concretas, se hará referencia a las

mismas mediante las siglas de su nombre y apellidos, evitando, por tanto, su identificación directa.

2. En general, los boletines y diarios oficiales tienen la consideración de fuentes accesibles al público, por lo que los datos personales allí publicados pueden ser utilizados por terceras personas sin necesidad de solicitar el consentimiento de las personas interesadas, siempre que no se vulneren sus derechos y libertades fundamentales. Por ello, deberá reducirse al mínimo suficiente para cumplir su finalidad la información de carácter personal que se incluya en los documentos a publicar.
3. El Ayuntamiento y sus entidades vinculadas o dependientes podrán ofrecer a la ciudadanía información sobre el personal a su servicio, que integre tanto el puesto de trabajo como el número de teléfono y la cuenta de correo electrónico, con el fin de facilitar a la ciudadanía la identidad de la persona con quien deba contactar para realizar una determinada gestión.

**Artículo 46. Publicidad en procesos de concurrencia competitiva y protección de datos.**

En los procedimientos de concurrencia competitiva, tales como la selección y provisión de personal al servicio del Ayuntamiento y de sus entidades vinculadas o dependientes, la concesión de subvenciones, etc., se podrá proceder a la publicación de datos personales relativos a personas físicas identificadas o identificables haciendo uso de medios electrónicos, cuando así lo establezcan las normas reguladoras de cada procedimiento, a cuyo efecto se advertirá acerca de esta publicación en las bases de selección o en la convocatoria aprobadas.

**Artículo 47. Petición de información por miembros de la Corporación y protección de datos.**

1. Todas las personas que integran la Corporación tienen derecho a obtener de la Presidencia de la misma cuantos antecedentes, datos o informaciones obren en poder de los servicios del Ayuntamiento y sus entidades vinculadas o

dependientes y resulten precisos para el desarrollo de su función de fiscalización y control de los órganos de gobierno de la misma, de conformidad con lo establecido en el artículo 77 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local. En este sentido, el artículo 11.2 a) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en relación con el anterior, ofrece la cobertura suficiente para que a las personas que integran la Corporación se les puedan facilitar datos personales.

2. Deberán comunicarse sólo aquellos datos de carácter personal que resulten adecuados, pertinentes y no excesivos en relación con la concreta finalidad de gobierno o de fiscalización y control que las personas como miembros de la Corporación tengan atribuida.
3. Cuando la información a suministrar contenga datos de carácter personal, se deberá valorar, en primer lugar, si es posible proceder a su disociación sin que ello afecte al derecho de los miembros de la Corporación a recibir la información necesaria para el ejercicio de sus funciones de control de los órganos de gobierno del Ayuntamiento o de sus entidades vinculadas o dependientes. Y, cuando esta opción no fuera posible por comprometer la comprensión de la información que deba suministrarse, se comunicará a quien deba recibir la información el deber de reserva y confidencialidad que le incumbe, respecto de la información de carácter personal que conozca en el ejercicio de su cargo.
4. A la entrega de la documentación, se recordará a las personas que son miembros de la Corporación que deberán observar el deber de confidencialidad de la información y de los datos de carácter personal a los que accedan en el ejercicio de su cargo representativo, aún después de finalizado su mandato.
5. La valoración de cuáles resulten ser esos datos, así como el cumplimiento de los requisitos de la solicitud y su motivación, corresponde en exclusiva a los correspondientes órganos de gobierno del Ayuntamiento.

#### **Artículo 48. Publicidad de los acuerdos de la Corporación.**

Se deberán facilitar a las personas que lo soliciten copias y certificaciones acreditativas de los acuerdos de la Corporación, aunque podrán retirarse de las mismas los datos de carácter personal, particularmente los especialmente protegidos, o aquellos que puedan afectar al derecho a la intimidad personal y familiar.

### **DISPOSICIONES ADICIONALES**

#### **Primera. Formación.**

El Ayuntamiento elaborará un plan anual de actividades informativas y acciones formativas dirigidas a todo su personal y de manera preferente, a quién trate datos personales y datos sensibles.

Asimismo, facilitará a su personal un decálogo que informe sobre los principios de la protección de datos, sus obligaciones y los derechos de la ciudadanía. El mismo se publicará en la intranet municipal y se adoptarán medidas para asegurar que todos los empleados públicos, especialmente los de nueva incorporación, tienen conocimiento del mismo.

#### **Segunda. Glosario.**

Los términos utilizados en el presente Reglamento se incorporarán al Glosario de Administración Electrónica previsto en la Ordenanza Municipal de Administración Electrónica.

### **DISPOSICIÓN TRANSITORIA ÚNICA**

#### **Formularios y modelos**

Con carácter normativo, y en el plazo de tres meses desde la entrada en vigor del presente Reglamento, el Ayuntamiento aprobará los formularios y modelos necesarios para relacionarse física o electrónicamente, en materia de protección de datos, con los ciudadanos, los empleados municipales, otras administraciones y, en lo que proceda, con la Agencia Española de Protección de Datos.

## DISPOSICIONES FINALES

### **Primera. Modificación y actualización del Reglamento.**

Las modificaciones y actualizaciones al presente Reglamento derivadas de cambios en la legislación sobre la materia serán aprobadas por el órgano competente. En particular, antes del 25 de mayo del 2018 el Ayuntamiento y sus entidades vinculadas o dependientes deben ser conformes con lo dispuesto en el 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 datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), de lo cual debe quedar reflejo en la pertinente modificación del presente Reglamento.

### **Segunda. Entrada en vigor.**

El presente Reglamento será objeto de aprobación y publicación de acuerdo con los trámites legales oportunos, se publicará en la sede electrónica del Ayuntamiento y en su portal de transparencia y entrará en vigor en el plazo establecido en el artículo 70.2 y 65 de la Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local, a partir de su publicación en el Boletín Oficial.