

## LA PROTECCION DE DATOS EN EL CORREO ELECTRÓNICO.

### LA CLÁUSULA PROTECCIÓN DE DATOS EN EL CORREO ELECTRÓNICO SEGÚN LA NUEVA NORMATIVA RGPD-LOPD

A la hora de enviar correos electrónicos a usuarios, ciudadanos, clientes o clientes potenciales, es necesario que estos cumplan con los requisitos exigidos por la normativa de protección de datos. Debe incluirse un texto o leyenda como **cláusula de protección de datos en el correo electrónico**.

Se define el **correo electrónico** como un servicio de la sociedad de la información que permite enviar y recibir mensajes con posibilidad de adjuntar todo tipo de contenidos digitales desde un ordenador o dispositivo móvil conectado a internet.

Segun la **Ley de Procedimiento Administrativo**<sup>1</sup> *“con independencia de que la notificación se realice en papel o por medios electrónicos, las administraciones públicas enviarán un aviso al dispositivo electrónico y/o a la dirección de correo electrónico del interesado que este haya comunicado, informándole de la puesta a disposición de una notificación en la sede electrónica de la administración u organismo correspondiente o en la dirección electrónica habilitada única. La falta de práctica de este aviso no impedirá que la notificación sea considerada plenamente válida» (LPAC, art. 41.6.).*

Por ello, no cabe duda de que la **dirección de correo electrónico personal**, e-mail profesional, de empresa o corporativo de los empleados/as es un dato de carácter personal<sup>2</sup>.

---

<sup>1</sup> Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas

<sup>2</sup> Segun el **Reglamento Europeo de Protección de Datos (RGPD)** son **datos personales**: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

**E-MAIL AMPARADO POR LA NORMATIVA DE PROTECCION DE DATOS.**

No podría dudarse de que la dirección de correo electrónico de las personas físicas o profesionales estén amparadas por la protección de datos y, por tanto de la **Ley Orgánica de Protección de Datos (LOPD-GDD)**<sup>3</sup> pues se tratan de datos personales.

En este sentido, cabe destacar que existen cuentas de correo electrónico que contienen datos de carácter de personal y en las cuales no existe ninguna duda de que estén amparadas por la LOPD. Entre esas direcciones de correos electrónicas están aquellas que contienen nombres, apellidos o fechas de nacimiento entre otras. Este tipo de cuentas o direcciones suponen, sin ningún tipo de duda, la inclusión de datos de carácter personal e identifican, incluso de forma directa, al titular del correo electrónico. Por ejemplo, *carmen.jimenez@...*, *perez.maria1982@...*, etc.

Por otra parte, existe un segundo supuesto en el cual, en principio, la dirección de correo electrónico no parece mostrar datos relacionados con la persona titular de la cuenta, como por ejemplo alias, pseudónimos o simples nombres genéricos (*luzdeldía@...*, *cpu12@...*, etc).

En este supuesto, un primer examen de la cuenta nos podría hacer concluir que no estamos ante un dato de carácter personal. Sin embargo, hay que tener presente que **la dirección del correo electrónico** siempre irá vinculada a un dominio concreto, por lo que se podrá identificar de manera no muy complicada al titular de la cuenta del correo electrónico( persona identificable) al servidor de dicho dominio.

Es decir, la mayoría de correos electrónicos generalistas pertenecen a plataformas como Yahoo, Gmail, Hotmail, Telefónica. Este tipo de correos son fáciles de rastrear y se podría llegar a identificar al titular del correo mediante la dirección IP con la cual se conectan al mismo. En consecuencia, cabe tener en consideración que el e-mail de una persona física siempre se tratará y tendrá condición de dato de carácter personal y por tanto, va a estar afectado por la citada Ley

<sup>3</sup> Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Orgánica de Protección de Datos (LOPD), y por tanto también, por el Reg

Es necesario recordar la importancia de proteger y respetar todo dato de carácter personal y en consecuencia, de hacer un uso responsable con las direcciones de correos electrónicos que tengamos en nuestro poder, para no llevar a cabo infracciones de la LOPD.

### **LA LEY PROTECCIÓN DE DATOS EN LOS CORREOS ELECTRÓNICOS**

Actualmente, la gran mayoría de las compañías, incluso Administraciones y empresas públicas recurren al **email marketing** para conseguir nuevos usuarios, suscriptores o clientes, además de usar el correo electrónico mayoritariamente para gran parte de sus comunicaciones con aquellos usuarios o clientes que ya tienen.

Sin embargo, a la hora de utilizar el email como medio de contacto con usuarios o clientes potenciales, es muy importante tener en cuenta las obligaciones que establece el **Reglamento Europeo de Protección de Datos (RGPD)**<sup>4</sup> respecto al email, es decir, debemos respetar la normativa de protección de datos al usar el correo electrónico como forma de comunicación.

En ese sentido, tanto el RGPD como la LOPD obligan a recabar el **consentimiento previo de los usuarios** para poder enviarles por email comunicaciones comerciales o de cualquier otra índole.

Este consentimiento para enviar publicidad a usuarios, suscriptores, clientes o clientes potenciales debe ser explícito, es decir, el usuario debe aceptarlo mediante una acción positiva, como puede ser marcar una casilla del tipo «*acepto recibir comunicaciones comerciales a través de email*».

Además, cuando se recaba el consentimiento para enviar correos electrónicos comerciales o para poder enviar las comunicaciones vía

---

<sup>4</sup> 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.

email, se debe informar a los usuarios de los aspectos básicos relativos al tratamiento de sus datos.

### **¿QUÉ ES LA CLÁUSULA DE PROTECCIÓN DE DATOS EN LOS CORREOS ELECTRÓNICOS?**

La **cláusula de protección de datos del email** es una cláusula de confidencialidad que alude a la privacidad y el deber de secreto que los destinatarios del email deben mantener respecto a la información contenida en el mismo.

Este **texto de protección de datos para email** suele emplearse en las comunicaciones entre personas o entidades que mantienen algún tipo de relación que exija mantener la confidencialidad de la información que comparten entre sí.

Existen modelos de comunicaciones para correo electrónico de acuerdo a la normativa de protección de datos para utilizar en las comunicaciones por email.

### **¿PARA QUÉ SIRVE EL TEXTO RGPD Y LOPD PARA EL CORREO ELECTRÓNICO?**

El texto **RGPD** y **LOPD** para correo electrónico sirve para cumplir con el deber de informar a los usuarios sobre el tratamiento de sus datos personales. Esta información se presenta en **una doble capa informativa**.

En **una primera capa** se debe suministrar esta información básica al usuario:

- Identidad del responsable del tratamiento
- Finalidad del tratamiento
- Legitimación o base jurídica
- Destinatarios de los datos
- Derechos del usuario y cómo ejercerlos
- Procedencia de los datos

## **DELEGADO PROTECCION DATOS. AYUNTAMIENTO ZARAGOZA**

---

- Plazo de conservación de los datos

En la **segunda capa** se profundizará en la información dada en la primera capa, aportando una información más completa sobre cada uno de esos elementos.

Esta misma información se suministrará al usuario, si se trata de un formulario para recabar el consentimiento para recibir comunicaciones comerciales por email o suscribirse a una newsletter, junto a la casilla marcada para que pueda dar dicho consentimiento expreso.

### **¿QUÉ DEBEN INCLUIR LOS TEXTOS LOPDGDD/RGPD DE LOS EMAILS?**

En el caso de la **cláusula de protección de datos**, el texto **LOPD para correo electrónico** puede seguir una fórmula básica similar a esta:

*«Esta comunicación va dirigida de manera exclusiva a su destinatario y puede contener información confidencial y/o sujeta a secreto profesional, cuya divulgación no está permitida por la Ley. Si ha recibido este mensaje por error, le rogamos que a la menor brevedad posible, se comuniqué mediante correo electrónico remitido a nuestra atención y proceda a su eliminación, así como cualquier documento adjunto al mismo».*

En cuanto al **texto LOPDGDD/RGPD** que debe incluir el email, antes de la cláusula de protección de datos (si la lleva) o después de la misma (lo cierto es que no hay una regla general para el orden de estos elementos), se puede poner un texto similar a este:

- En cumplimiento del **RGPD** en materia de protección de datos personales, le informamos de que recibe este email por estar suscrito a (XXXXXX).
- El **responsable del tratamiento de sus datos** es (XXXXXX), con NIF (XXXXXX) y domicilio fiscal (XXXXXX).
- La **finalidad** para la que se recogen sus datos es (XXXXXX) (por ejemplo, para enviarle la newsletter mensual de acuerdo a su solicitud de suscripción).

- **Período de conservación de los datos.** Su información permanecerá en nuestra base de datos durante (XX semanas/meses/año) y que no será cedida a terceros.
- **Ejercicio de derechos.** Puede ejercer sus derechos de acceso, rectificación, cancelación, oposición o limitación del tratamiento poniéndose en contacto con nosotros a través de (XXXXXX)».

### **¿CÓMO PONER LEYENDA PROTECCIÓN DE DATOS EN EL CORREO ELECTRÓNICO?**

Tanto el **texto LOPDGDD/RGPD** como la **cláusula de protección de datos en el correo electrónico** puede incorporarse de manera sencilla en cualquier servidor de correo, puesto que puede incluirse como la firma predefinida o predeterminada al final del campo de texto del email.

A modo de ejemplo, si se usase **Gmail**, se siguen estos pasos para incluir estos textos de protección de datos para el correo electrónico:

- En tu cuenta de Gmail, entra en «Configuración» (tendrás que pulsar en el icono del engranaje en la esquina superior derecha)
- Pulsa en «Ver todos los ajustes» en el menú que se desplegará
- En la pantalla a la que accederás, sin salir de la pestaña «General», baja hasta que veas la opción de «Firma»
- Pulsa en «Crear»
- Ponle un nombre a la firma, por ejemplo, LOPD
- Escribe los textos LOPDGDD/RGPD y la cláusula de privacidad en la caja de texto, dándoles el formato que desees con las opciones de edición que tienes a tu disposición
- Para que aparezca esta firma, tendrás que elegirla en los «Valores predeterminados de firma» que aparecen justo bajo la caja de texto. Pulsa en los menús desplegables y elige la firma LOPD que has creado

## **DELEGADO PROTECCION DATOS. AYUNTAMIENTO ZARAGOZA**

---

- Finalmente, baja hasta el final y pulsa en «Guardar cambios»

Con otros servidores de correo electrónico el proceso es muy similar, solo tienes que localizar la «Firma» en la configuración del correo, escribir en ella los textos LOPDGDD/RGPD para emails y guardar los cambios.

### **IMPLEMENTACIÓN DE LA LEY DE PROTECCIÓN DE DATOS EN CORREO ELECTRÓNICO 2021: APLICACIÓN, CLÁUSULA Y TEXTO PARA INSERTAR**

Cumplir con la normativa de protección de datos es obligatorio a la hora de recabar información o establecer cualquier comunicación con usuarios, clientes, empleados o proveedores. Esto incluye el envío de emails.

### **Ley de Protección de Datos en los correos electrónicos. ¿Cómo afecta al envío de emails?**

Actualmente las empresas y organizaciones utilizan el email marketing para conseguir nuevos leads o suscriptores. Esta estrategia se basa en el envío de newsletters y correos electrónicos comerciales a los usuarios que hayan aceptado recibir dicha información expresamente.

Pero, ¿qué pasa con la entrada en vigor del **Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de datos (LOPDGDD)**?

Estas nuevas normativas afectan directamente a los requisitos para manejar datos de usuarios y enviarles boletines informativos, promociones u ofertas a través del email. Y hay una palabra clave para entender cómo adaptar una **newsletter al RGPD**: consentimiento.

Hasta ahora el consentimiento de los usuarios se podía obtener de una forma “tácita”. Por ejemplo, al aceptar la política de privacidad (el típico “*He leído y aceptado las políticas de privacidad*”) el usuario también estaba autorizando a que le enviaran correos electrónicos. Sin embargo, ahora el consentimiento debe ser explícito.

## **DELEGADO PROTECCION DATOS. AYUNTAMIENTO ZARAGOZA**

---

Esto ha afectado también al diseño de formularios de contacto. Hasta ahora, los formularios eran mucho más simples. Una simples casillas donde introducir los datos básicos. Sin embargo, ahora el **texto LOPD para correo electrónico** debe incluir una serie de información básica, presentada en una doble capa informativa.

Por otra parte, está la obligación de hacer una reestructuración de las bases de datos. El RGPD no considera válidos aquellos suscriptores obtenidos de formas no previstas por la actual ley. Las empresas que hayan obtenido los clientes de forma no lícita, deberán volver a enviarles un correo informando sobre la obligación del cliente de volver a prestar su consentimiento, esta vez de forma explícita y de acuerdo al RGPD.

En definitiva, podemos decir que la **LOPD y el RGPD** afectan al envío de correos electrónico en tres aspectos:

- Obligación de informar (doble capa informativa)
- Obtención de consentimiento explícito
- Depurar y renovar las bases de datos
- No olvides que los usuarios pueden apuntarse a la Lista Robinson para impedir que las empresas les envíen información por email, correo ordinario, teléfono móvil o fax.

### **TEXTOS RELATIVOS al RGPD y la LOPD para el CORREO ELECTRÓNICO.**

Para cumplir con la **protección de datos en el correo electrónico**, reiteramos que los emails han de cumplir con la obligación de presentar una doble capa informativa.

En **la primera capa** se informa de forma básica sobre:

- Identidad del responsable del tratamiento
- Finalidad y plazo de conservación de datos
- Base jurídica
- Destinatarios de la información
- Derechos del usuario

## **DELEGADO PROTECCION DATOS. AYUNTAMIENTO ZARAGOZA**

---

- Procedencia de la información

Se debe incluir una segunda capa informativa en la que se profundice en estos datos. Por ejemplo, respecto a la identidad del responsable, se ampliarán los datos ya presentados o sobre la identidad del representante o del delegado de protección de datos, si lo hubiese.

La **LOPD en newsletter** también obliga a incluir en los formularios un método para que el usuario pueda prestar su consentimiento explícito, inequívoco y voluntario. Por ejemplo, con la inclusión de una check box o casilla de aceptación y un captcha (para demostrar que el usuario no es un bot).

### **La cláusula de protección de datos en el correo electrónico**

También es necesario que los correos electrónicos incluyan una **cláusula de confidencialidad** para salvaguardar la privacidad y confidencialidad de la información y garantizar que los destinatarios mantengan el deber de secreto del contenido comunicado por ese conducto.

Esta **cláusula de protección de datos en el correo electrónico** se suele emplear en aquellos casos en los que remitente y destinatario tienen firmado algún acuerdo de confidencialidad, con el objetivo de funcionar como un recordatorio de dicho acuerdo.

### **Algunos ejemplos:**

**Advertencia legal: ESTE CORREO ELECTRÓNICO PUEDE CONTENER INFORMACIÓN CONFIDENCIAL REFERENTE A PERSONAS FÍSICAS.**

Esta información está protegida por la Constitución española y por la Ley Orgánica de Protección de Datos. La OFICINA DE RRHH DEL EXCMO. AYUNTAMIENTO DE ZARAGOZA cuenta con un sistema de protección de datos implementado que tutela los derechos de las personas físicas. Es por ello que la información transmitida al destinatario está habilitada por la legislación vigente y/o autorizada expresamente por el propio interesado. Usted como destinatario será responsable exclusivo del tratamiento y de la seguridad de la información transmitida una vez registrada en sus sistemas de información. En el caso de recibir información protegida por claves de acceso, por motivos de seguridad y para garantizar que es usted el destinatario real de la información, póngase en contacto con el emisor de este correo.

## **DELEGADO PROTECCION DATOS. AYUNTAMIENTO ZARAGOZA**

---

Este mensaje y, en su caso, los ficheros anexos tienen carácter confidencial, y se dirigen exclusivamente al destinatario referenciado. Si usted no lo es y lo ha recibido por error o tiene conocimiento del mismo por cualquier motivo, le rogamos que nos lo comunique por este medio y proceda a destruirlo o borrarlo, y que en todo caso se abstenga de utilizar, reproducir, alterar, archivar o comunicar a terceros el presente mensaje y ficheros anexos, todo ello para evitar incurrir en responsabilidades legales.

En virtud de lo establecido en la normativa sobre Protección de Datos de carácter Personal, la Oficina de RRHH del Excmo. Ayuntamiento de Zaragoza (responsable del fichero de contactos) comunica que la información del destinatario de correo electrónico se utiliza para mantener la comunicación entre ambas partes, así como para la gestión de correos y contactos de nuestra entidad. Puede ejercer los derechos de acceso, rectificación, cancelación y oposición en cualquier momento en Edificio del Seminario, Vía Hispanidad nº 20, 50071, Zaragoza o en [lopdrecursoshumanos@zaragoza.es](mailto:lopdrecursoshumanos@zaragoza.es)

### **ADVERTENCIA LEGAL:**

Este mensaje va dirigido, de manera exclusiva, a su destinatario y puede contener información confidencial y sujeta al secreto profesional, cuya divulgación no está permitida por Ley. Se realiza en el ejercicio de funciones legales previstas en el REGLAMENTO GENERAL DE PROTECCION DE DATOS (RGPD), y en la Ley Orgánica de P.D.. Se encuentra amparada por el artículo 18.3 de la Constitución que recoge el derecho al secreto de las comunicaciones. En caso de haber recibido este mensaje por error, le rogamos que de forma inmediata, nos lo comunique mediante correo electrónico remitido a nuestra atención y proceda a su eliminación, así como a la de cualquier documento adjunto al mismo. Asimismo, le comunicamos que la distribución, copia o utilización de este mensaje, o de cualquier documento adjunto al mismo, sin autorización expresa, cualquiera que fuera su finalidad, pueden estar prohibidas por la Ley. Puede ejercer sus derechos establecidos en la citada normativa, en esta dirección de correo electrónico.

### **AVISO LEGAL**

El contenido de este correo electrónico, y sus anexos, son estrictamente confidenciales, secretos y restringidos. La divulgación o el suministro, en todo o en parte, a cualquier tercero, no podrá ser realizada sin el previo, expreso y escrito consentimiento de ACTORA CONSUMO (Asociación de Consumidores Torre Ramona). Las opiniones contenidas en este mensaje y en los archivos adjuntos, pertenecen exclusivamente a su remitente y no representan la opinión de ACTORA CONSUMO, salvo que se diga expresamente y el remitente esté autorizado para ello. ACTORA CONSUMO, advierte

## **DELEGADO PROTECCION DATOS. AYUNTAMIENTO ZARAGOZA**

---

expresamente que el envío de correos electrónicos a través de Internet no garantiza, ni la confidencialidad de los mensajes, ni su integridad y correcta recepción, por lo que ACTORA CONSUMO, no asume responsabilidad alguna por dichas circunstancias. En caso que no sea el destinatario, y haya recibido este mensaje por error, agradecemos lo comunique inmediatamente al remitente sin difundir, almacenar o copiar su contenido.

### **NOTA INFORMATIVA PROTECCION DATOS PERSONALES.**

- Los datos personales aportados en la consulta/queja/reclamación o denuncia de consumo formulada por usted en este correo electrónico no generan ningún procedimiento administrativo, serán incorporados a un fichero denominado **CONSULTAS OMIC** que gestiona esta Oficina como encargado del tratamiento, utilizados, de forma confidencial, para contestarle mediante servicios de información y asesoramiento, dentro de las funciones que atribuye a las **OMIC** la Ley 16/2006, de 28 de diciembre, de Protección y Defensa de los Consumidores y Usuarios de Aragón, y la Ley 10/2017, de 30 de noviembre, de Régimen especial del municipio de Zaragoza como capital de Aragón.
- Los datos, una vez registrados, se conservarán durante un plazo máximo de un año, y serán utilizados de forma anonimizada y disociados con fines estadísticos e informativos, para insertar los resultados en la Memoria de gestión anual de la **OMIC**.
- De conformidad con lo establecido en el Reglamento (UE) 2016/679 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 en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los derechos digitales se le informa que podrá usted ejercer los derechos de acceso, rectificación, oposición y cancelación de sus datos en la forma establecida por la ley, mediante comunicación ante esta **Oficina** en la siguiente dirección: **OMIC-Ayuntamiento de Zaragoza**, Vía Hispanidad nº20, **Centro Administrativo EL SEMINARIO**, planta sótano -1, 50009 Zaragoza; y accediendo, en su caso, a la cuenta de correo electrónico [omic@zaragoza.es](mailto:omic@zaragoza.es).

### **¿Qué texto LOPD y RGPD deben incluir los correos electrónicos?**

**¿Cómo poner en el correo la protección de datos?** Se puede mostrar con un ejemplo práctico:

## **DELEGADO PROTECCION DATOS. AYUNTAMIENTO ZARAGOZA**

---

*“Para cumplir con el RGPD en materia de protección de datos personales, le informamos como usuario que el responsable del tratamiento de sus datos es XXXXX, con NIF XXXXX y domicilio fiscal en XXXXX.*

*La finalidad por la que recogen sus datos es XXXXX (ejemplo, “proponerle ofertas comerciales de acuerdo a sus intereses”).*

*También le informamos de que su información permanecerá en nuestra base de datos durante XXXXX tiempo y que ésta no será cedida a terceros.*

*Puede ejercer sus derechos de acceso, rectificación, cancelación, oposición o limitación del tratamiento poniéndose en contacto con nosotros a través de XXXXX“.*

En caso de ser necesario incluir una cláusula de protección de datos en el correo electrónico relacionada con la confidencialidad, se podría añadir en el pie del mensaje un texto similar a este:

*“Esta comunicación contiene información confidencial y privilegiada de uso exclusivo para el destinatario/s del mensaje. Si usted no es el destinatario/s tenga en cuenta que cualquier distribución, copia o uso de esta comunicación queda totalmente prohibida. Si usted ha recibido esta comunicación por error por favor notifíquelo a la mayor brevedad por correo electrónico o por teléfono”.*

### **¿Cómo insertar el texto de LOPD en los correos electrónicos?**

A nivel informativo podemos ver cómo insertar este **aviso de protección de datos en el correo electrónico** en los servicios de mensajería más conocidos.

### **Cómo insertar una clausula LOPD/RGPD en Gmail**

Si quieres incluir un **texto legal correo en el electrónico de Gmail**, sigue estos pasos:

1. Inicia sesión en tu cuenta Gmail.

## **DELEGADO PROTECCION DATOS. AYUNTAMIENTO ZARAGOZA**

---

2. Haz click en el botón de *configuración* (representado con un dibujo de un engranaje) en la esquina superior derecha
3. Selecciona “*Configuración*” en el menú que se despliega.
4. Se abrirá la pantalla de configuración en la pestaña “*General*”. Sin cambiar de pestaña, baja hasta encontrar la sección “*Firma*”.
5. Escribe el aviso de LOPD en la caja de texto que aparece. Puedes darle el formato que prefieras con las herramientas que te proporciona.
6. Guarda la configuración haciendo click en el botón “Guardar cambios” al final de la pantalla.

### **Cómo insertar una firma RGPD en Hotmail**

Para insertar un **texto de protección de datos en email** de Hotmail, has de hacer o siguiente:

1. Inicia sesión en tu cuenta Hotmail.
2. Pulsa el botón de *configuración* (representado con un dibujo de un engranaje) en la esquina superior derecha.
3. Selecciona “*Opciones*” en el menú que aparece.
4. En la pantalla de Opciones, haz click en “*Formato, fuente y firma*” que aparece en la sección “*Escribir correo electrónico*”.
5. Escribe el texto LOPD en el espacio proveído para la firma. Utiliza el formato que prefieras para ello.
6. Pulsa el botón “*Guardar*” para conservar los cambios.

### **Como insertar el texto legal en Yahoo**

1. Inicia sesión en tu cuenta Yahoo.
2. Haz click en el botón de *configuración* (representado con un dibujo de un engranaje) en la esquina superior derecha.

## **DELEGADO PROTECCION DATOS. AYUNTAMIENTO ZARAGOZA**

---

3. En la ventana que emerge, selecciona “*Escribiendo mensaje*”, en la columna de la izquierda.
4. En el apartado “*Firma*” puedes elegir escribir el texto con o sin formato.
5. Escribe el texto LOPD y pulsa el botón “*Guardar*”.

### **Como insertar una firma en Microsoft Outlook**

1. Haz click en “*Herramientas*”, en el menú superior.
2. Selecciona “*Opciones...*”.
3. En la ventana que emerge, pulsa sobre la pestaña “*Formato de correo*”.
4. Haz click sobre el botón “*Firmas...*”.
5. En la nueva ventana que aparece, mantente en la pestaña “*Firma de correo electrónico*”. Pulsa el botón “*Nueva*” y asígnale un nombre.
6. Escribe el texto LOPD en el espacio proporcionado. Puedes darle el formato que quieras.
7. Haz click en “*Aceptar*” para guardar la configuración.

### **Como insertar el texto LOPD en ThunderBird**

1. Dentro de ThunderBird, accede a “*Herramientas*” y, a continuación en “*Configuración de las cuentas*”
2. Selecciona la cuenta de correo que vas a configurar, por si tienes más de una, en el menú de la izquierda
3. Pasamos a la parte derecha, en el recuadro “*Texto de la firma*” introduce el texto de protección de datos a incluir en los correos electrónicos
4. Por último “*Aceptar*”

### **LA PRIVACIDAD EN EL CORREO ELECTRÓNICO**

El correo electrónico es una herramienta que millones de personas utilizan todos los días para comunicarse, ya sea a nivel personal o laboral. En las Administraciones públicas es ya habitual hacerlo tanto externa como internamente.

La mayoría de plataformas de correo electrónico cuentan con soluciones tecnológicas para garantizar la seguridad y privacidad de las direcciones de correo electrónico y los mensajes, como por ejemplo el cifrado de extremo a extremo.

Sin embargo, garantizar la **privacidad en el correo electrónico** también es responsabilidad del propio usuario, por ejemplo utilizando contraseñas seguras, o no dejando las credenciales a la vista cuando utiliza un equipo.

### **¿Cómo garantizar mi privacidad en el correo electrónico de empresa?**

En el caso en el que se use un **correo electrónico de trabajo**, también hay que adoptar una serie de medidas de seguridad, que exponemos en forma de consejos prácticos:

- No usar el mismo correo electrónico en el ámbito laboral que el que se utiliza en el ámbito personal.
- Usar contraseñas seguras, con un mínimo de ocho caracteres, con una combinación de mayúsculas, minúsculas, números y símbolos.
- Evitar el uso de nombres o contraseñas fáciles de adivinar, como el nombre de usuario o de la empresa.
- Cambiar la contraseña de forma periódica.
- Cerrar siempre la sesión y la página de correo electrónico para evitar que lo puedan ver tercero, sobre todo cuando se accede al correo desde un equipo distinto al habitual.
- Utilizar servicios que permitan protección contra la pérdida de datos o acceso a la información cuando se produzca una caída del servidor.
- Complementar el almacenamiento en servidores externos con el almacenamiento en local, de manera que no se dependa

totalmente del buen funcionamiento de estos servidores externos.

### **La privacidad en el envío de correos masivos en el trabajo.**

La **información sobre el correo electrónico se consideran datos personales**, por lo que la empresa o Administración pública debe hacer todo lo que esté en su mano para garantizar su privacidad. No hay problema cuando se trata de compartir direcciones de usuario electrónico entre personas conocidas.

Pero, ¿qué pasa cuando el **correo electrónico en la empresa se usa para enviar mails múltiples a personas que no se conocen entre sí?**

Esto es frecuente en las empresas y organizaciones, ya que en muchos casos se envía información común para proveedores, clientes o prestadores de servicios.

¿Cómo enviar correos masivos sin desvelar las direcciones de correo de los destinatarios? Usando la copia oculta o Cco.

Al enviar correos masivos con copia oculta, el destinatario de dicha información no puede saber si se ha añadido más gente al campo Cco. A su vez, las personas incluidas en **copia oculta** no pueden ver las direcciones de correo del resto de usuario incluidos en el campo. La mayoría de servicios de correo electrónico permiten activar la opción de enviar copia oculta en el campo de los destinatarios del email.

El correo profesional, que antes era el único canal de información interna en muchas entidades, ha dejado paso a **las plataformas tecnológicas de productividad y ofimática en la nube**. A través de estas plataformas fluye una gran parte de la información de la organización, en particular, datos de carácter personal y, en los últimos tiempos, las plataformas se han convertido en uno de los activos más interesantes para los ciberdelincuentes por la posibilidad de acceder a información estratégica y confidencial.

### I.-Correo electrónico y plataformas de productividad y ofimática en la nube

El correo electrónico, desde su invención en la década de 1960, se ha ido popularizando a la vez que las redes y servicios de comunicaciones de datos se iban haciendo más accesibles. En la actualidad sigue siendo en una de las herramientas de comunicación más usadas, tanto en el ámbito laboral como en el privado.

En la arquitectura tradicional, el correo electrónico se encontraba alojado en los servidores de la organización y estaba administrado por personal propio o externo. Con la introducción de las nuevas tecnologías, como la mensajería instantánea o las redes sociales, el escenario es diferente. Ahora se usan los recursos computacionales en la nube que proporcionan las grandes multinacionales tecnológicas.

El correo electrónico ha crecido también en funcionalidad. Si antes era un simple medio de intercambio de mensajes de texto, ahora constituye una parte clave del proceso de toma de decisiones de la organización al haber añadido funcionalidades extra como compartición de documentos en la nube, videoconferencia, encuestas, multimedia, etc.

Como resultado de esta evolución, las entidades han acumulado grandes repositorios de información en la nube. Normalmente, estos almacenes están accesibles con las mismas credenciales del correo electrónico. La nube almacena y procesa información actualizada, y también histórica, de organizaciones públicas y privadas de cualquier ámbito, desde pequeñas empresas a **grandes compañías**, pasando por **centros educativos**.

Entre las plataformas más usadas pueden citarse productos como Office365 de Microsoft, o Google Suite que actualmente copan el mercado en los entornos profesionales.

### II.-Riesgos para la privacidad

El **acceso a las plataformas de productividad online** también ha evolucionado. Al principio era necesario utilizar el ordenador

## DELEGADO PROTECCION DATOS. AYUNTAMIENTO ZARAGOZA

---

corporativo conectado a la intranet para acceder al correo electrónico. Ahora, sin embargo, es posible acceder desde cualquier dispositivo con conexión a internet que tengamos a nuestro alcance, independientemente de la red a la que estemos conectados. En la mayor parte de los casos, ya no se requiere disponer de una aplicación específica para el acceso, basta simplemente con un navegador web, y una única dirección común para el acceso de los empleados de todas las organizaciones que utilicen la misma plataforma corporativa. Esta es una de las ventajas de tener la información en la nube, pero a su vez un riesgo inherente a esta tecnología.

Debido a esta facilidad para conectarse, y que la superficie de ataque a estos sistemas sea todo Internet, pueden enumerarse, entre otros, las siguientes amenazas:

- Intentos de acceso a plataformas corporativas por fuerza bruta.
- Intentos de acceso a través de la reutilización de las credenciales en otros servicios de Internet que han sido objeto de una brecha de seguridad.
- Robo de las credenciales a través de ataques de ingeniería social como el phishing, que acaban dando por resultado que el usuario introduzca sus credenciales corporativas en páginas fraudulentas controladas por los ciber atacantes.
- Exposición de información personal al no diferenciar las herramientas empleadas en el entorno laboral del entorno privado.

El responsable del tratamiento ha de adoptar medidas para minimizar la probabilidad de que se materialicen las amenazas anteriores. Entre otras, podemos destacar:

- Elegir soluciones y prestadores de servicio confiables y con garantías, y prestar atención a la configuración de las opciones de seguridad y privacidad que ofrecen las plataformas de productividad en la nube.
- Establecer procedimientos y recomendaciones de acceso a las herramientas corporativas en movilidad y teletrabajo, que sean

fácilmente entendibles y ejecutadas por todos los miembros de nuestra organización.

- Establecer políticas restrictivas de acceso a las herramientas de productividad corporativas para uso personal o desde dispositivos no corporativos. En caso de permitirlo, establecer medidas de seguridad apropiadas y mecanismos de compartimentación de la información que mantengan separados el ámbito personal del profesional.
- Usar un segundo factor de autenticación: esta es la medida más recomendada en acceso a servicios online. Las suites de ofimática online suelen contar con la posibilidad de no sólo acceder con usuario y contraseña, sino añadir robustez a la autenticación mediante un token, un mensaje SMS o el uso de una APP en otro dispositivo.
- Emplear contraseñas robustas: el uso de contraseña difíciles de predecir y que no se usen en otros servicios es fundamental para protegerse de acceso indebidos. Es necesario implementar una correcta política de uso de contraseñas en la organización. Es recomendable consultar los servicios que nos informan de las cuentas que han sufrido brechas de seguridad en otras webs por si algún miembro de la organización ha reutilizado sus credenciales.
- Comprobar los accesos indebidos: realizar una gestión correcta de los registros de acceso a estos portales nos puede dar mucha información, como accesos producidos durante horas en las que no se debería acceder, direcciones IP geolocalizadas en lugares sin presencia de la organización, o constantes errores de acceso en algunas cuentas. Estos rastros nos darán las pistas necesarias para saber si nuestra organización está siendo objeto de algún tipo de ataque.
- Comprobar las redirecciones en los buzones de correo: una vez que se han comprometido las credenciales de acceso, una de las primeras acciones que realizan los ciberdelincuentes es crear una regla de redirección de correo para intervenir nuestras comunicaciones, reenviándose a un buzón propio los correos que recibimos. De esta manera, los atacantes pueden analizar la información sin tener que estar accediendo a nuestro buzón. Dependiendo de la plataforma de productividad usada,

es posible comprobar esta amenaza de diferentes maneras. Por ejemplo, un administrador puede usar esta solución para Office365. En cualquier caso, los usuarios siempre tienen la opción de consultar si tienen alguna regla y eliminarla.

### **Reglas de redirección de correo en Office 365.**

- Formar a los integrantes de la organización pública en la cultura de la protección de datos y seguridad. Debe hacerse hincapié en la necesidad de proteger las credenciales y erradicar su reutilización. También es preciso hablar de las amenazas basadas en ingeniería social, para evitar que los empleados introduzcan sus credenciales en páginas de inicio de sesión falsas.
- Establecer políticas de cancelación o bloqueo periódico de datos.
- Establecer sistemas de auditoría automática que alerten de acciones anómalas sobre el sistema de correo y paralicen ciertas actividades.

Este post forma parte de una serie sobre **brechas de seguridad**, entre los que se encuentran:

- Brechas de seguridad de datos personales: protégete ante la pérdida o robo de un dispositivo portátil
- Brechas de seguridad de datos personales: qué son y cómo actuar
- Brechas de seguridad de datos personales: protégete ante el ransomware
- Brechas de seguridad de datos personales: comunicación a los interesados
- Brechas de seguridad de datos personales: El Top 5 de las medidas técnicas que debes tener en cuenta

### **Comunicaciones comerciales por vía electrónica<sup>5</sup>**

#### Artículo 19. **Régimen jurídico.**

1.-Las comunicaciones comerciales y las ofertas promocionales se regirán, además de por la **Ley 34/2002**, por su normativa propia y la vigente en materia comercial y de publicidad.

2.-En todo caso, será de aplicación la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (derogada)<sup>6</sup>, y su normativa de desarrollo, en especial, en lo que se refiere a la obtención de datos personales, la información a los interesados y la creación y mantenimiento de ficheros de datos personales.

#### Artículo 20.-**Información exigida sobre las comunicaciones comerciales, ofertas promocionales y concursos.**

1.-Las comunicaciones comerciales realizadas por vía electrónica deberán ser claramente identificables como tales, y la persona física o jurídica en nombre de la cual se realizan también deberá ser claramente identificable.

2.-En los supuestos de ofertas promocionales, como las que incluyan descuentos, premios y regalos, y de concursos o juegos promocionales, previa la correspondiente autorización, se deberá asegurar, además del cumplimiento de los requisitos establecidos en el apartado anterior y en las normas de ordenación del comercio, que queden claramente identificados como tales y que las condiciones de acceso y, en su caso, de participación sean fácilmente accesibles y se expresen de forma clara e inequívoca.

3.-Lo dispuesto en los apartados anteriores se entiende sin perjuicio de lo que dispongan las normativas dictadas por las Comunidades Autónomas con competencias exclusivas sobre consumo.

4.-En todo caso, queda prohibido el envío de comunicaciones comerciales en las que se disimule o se oculte la identidad del remitente por cuenta de quien se efectúa la comunicación o que contravengan lo dispuesto en este artículo, así como aquéllas en las que se incite a los destinatarios a visitar páginas de Internet que contravengan lo dispuesto en este artículo.

---

<sup>5</sup> Ley 34/2002, de 11 de julio, de **Servicios de la sociedad de la información y de comercio electrónico.**

<sup>6</sup> Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los derechos digitales

## **DELEGADO PROTECCION DATOS. AYUNTAMIENTO ZARAGOZA**

---

### **Artículo 21.-Prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes.**

1.-Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

2.-Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.

Cuando las comunicaciones hubieran sido remitidas por correo electrónico, dicho medio deberá consistir necesariamente en la inclusión de una dirección de correo electrónico u otra dirección electrónica válida donde pueda ejercitarse este derecho, quedando prohibido el envío de comunicaciones que no incluyan dicha dirección.

### **Artículo 22.-Derechos de los destinatarios de servicios.**

1.-El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente.

A tal efecto, los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado. Cuando las comunicaciones hubieran sido remitidas por correo electrónico dicho medio deberá consistir necesariamente en la inclusión de una dirección de correo electrónico u otra dirección electrónica válida donde pueda ejercitarse este derecho quedando prohibido el envío de comunicaciones que no incluyan dicha dirección.

Asimismo, deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos.

2.-Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley

## **DELEGADO PROTECCION DATOS. AYUNTAMIENTO ZARAGOZA**

---

Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (derogada)<sup>7</sup>.

Cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento de los datos podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones.

Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.

### **Artículo 14.-Derecho y obligación de relacionarse electrónicamente con las Administraciones Públicas<sup>8</sup>.**

1.-Las personas físicas podrán elegir en todo momento si se comunican con las Administraciones Públicas para el ejercicio de sus derechos y obligaciones a través de medios electrónicos o no, salvo que estén obligadas a relacionarse a través de medios electrónicos con las Administraciones Públicas. El medio elegido por la persona para comunicarse con las Administraciones Públicas podrá ser modificado por aquella en cualquier momento.

2. En todo caso, estarán obligados a relacionarse a través de medios electrónicos con las Administraciones Públicas para la realización de cualquier trámite de un procedimiento administrativo, al menos, los siguientes sujetos:

- a) Las personas jurídicas.
- b) Las entidades sin personalidad jurídica.
- c) Quienes ejerzan una actividad profesional para la que se requiera colegiación obligatoria, para los trámites y actuaciones que realicen con las Administraciones Públicas en ejercicio de dicha actividad profesional. En todo caso, dentro de este colectivo se entenderán incluidos los notarios y registradores de la propiedad y mercantiles.
- d) Quienes representen a un interesado que esté obligado a relacionarse electrónicamente con la Administración.

---

<sup>7</sup> Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

<sup>8</sup> Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas

e) Los empleados de las Administraciones Públicas para los trámites y actuaciones que realicen con ellas por razón de su condición de empleado público, en la forma en que se determine reglamentariamente por cada Administración.

3. Reglamentariamente, las Administraciones **podrán establecer la obligación de relacionarse con ellas a través de medios electrónicos** para determinados procedimientos y para ciertos colectivos de personas físicas que por razón de su capacidad económica, técnica, dedicación profesional u otros motivos quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios.

### **Correo electrónico: la legislación que regula los emails**

El aumento de la visibilidad, la mejora de la publicidad, el análisis más rápido de los resultados, la medición de datos... son algunos de los motivos que justifican que los negocios y la Administración apuesten por la vía telemática para sus comunicaciones. Además, muchas de estas iniciativas reducen considerablemente la inversión en publicidad, sin que se sacrifiquen los resultados, sino, más bien, todo lo contrario.

### **Campañas de marketing de correo electrónico. Legislación**

Existen muchas cuestiones a considerar para realizar una campaña de marketing por correo electrónico, además de los aspectos sobre la publicidad y el enfoque, no hay que olvidar los aspectos legales y la protección de los datos y la privacidad del usuario.

### **¿Qué hay que saber sobre enviar correo electrónico con publicidad?**

#### **Identificación del carácter comercial**

Todo correo electrónico enviado por una empresa a uno o varios usuarios, debe incluir información específica y clara al hecho de que el contenido del mensaje tiene una finalidad promocional: de la empresa, de productos, de ofertas...

### **¿Qué requisitos deben cumplir los correos publicitarios?**

Según la Ley de Protección de Datos los correos electrónicos comerciales deben cumplir las siguientes normas:

- indicar de forma clara la finalidad del mensaje,
- ofrecer la posibilidad al destinatario de oponerse al tratamiento de sus datos con fines promocionales de forma gratuita y sencilla y
- proveer a los receptores de una dirección de correo electrónico válida para poder revocar en cualquier momento el consentimiento otorgado.

### **Gestión y Divulgación de datos de carácter personal**

Uno de los aspectos en los que más se ha incidido en los últimos años en materia de correo electrónico y comercio online es en la correcta gestión de los datos privados de los usuarios. De acuerdo, con la ley es necesario poner los medios suficientes para que terceras personas no puedan acceder a los datos cedidos por un usuario a una empresa, salvo que este haya dado su consentimiento expreso.

### **Derecho al honor, a la privacidad y a la protección de imagen<sup>9</sup>**

Son derechos que se encuentran en la Constitución y que, por lo tanto, en el entorno digital se extiende este derecho, que garantiza la privacidad de las comunicaciones de tipo comercial que se hicieran entre la empresa y el cliente.

### **Derecho de modificación y cancelación de datos**

---

<sup>9</sup> Artículo 18.1. de la Constitución. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

Está previsto por la ley que, en todo momento, el usuario pueda tener el libre acceso a los datos proporcionados a la empresa. Es decir, que el cliente tiene la potestad para acceder a los datos que la empresa tiene, modificarlos e, incluso, a cancelarlos.

Para que se cumplan los derechos de los usuarios de cuentas de correo, existen distintos organismos y asociaciones que vigilan el cumplimiento de las normas aplicables.

### **Correo electrónico de empleados de la empresa. Legislación.**

Del mismo modo que existe una legislación sobre los correos electrónicos comerciales, también se aplica una legislación al correo electrónico de la empresa proporcionado por una empresa a sus trabajadores, con el fin de facilitar las comunicaciones profesionales.

En este caso, hay que tener en cuenta el tipo de contrato y las condiciones en las que se firmó el mismo, así como qué indican los convenios de la empresa o del sector en cuanto a los usos del correo electrónico de empresa.

### **¿Y sobre los correos electrónicos de los empleados?**

#### **Uso para fines profesionales**

En las empresas y Administraciones, debe establecerse una, o varias cláusulas en las que se indica que el correo electrónico de la empresa tiene carácter profesional y que, en este sentido, se debe usar solo para comunicaciones empresariales propias del cargo que el trabajador ocupa.

#### **Limitación de la privacidad del correo de empresa<sup>10</sup>**

---

<sup>10</sup> Artículo 87 LOPD-GDD. **Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.**

1. Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.

2. El empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la

## **DELEGADO PROTECCION DATOS. AYUNTAMIENTO ZARAGOZA**

---

Uno de los aspectos más cuestionados de los últimos años es el derecho a la privacidad de los correos electrónicos de los trabajadores. En la actualidad, se entiende que la empresa puede tener acceso al contenido de los emails de los trabajadores cuando tenga sospechas de comportamientos poco éticos.

El uso indebido de correo electrónico de la empresa por parte de un trabajador podría ser causa suficiente para un despido procedente. Sin embargo, existen a que se tienen que dar para que la empresa tenga acceso a emails o conversaciones que puedan ser sospechosas, o lo que es lo mismo, no se pueden realizar situaciones de control indiscriminadas sobre el contenido de los emails de empleados.

### **Mayor protección de los usuarios**

La utilización de Internet como medio de comunicación de las empresas ha aumentado la protección de los usuarios frente a los correos comerciales y el marketing, asegurando un mayor control de la gestión de los datos y más seguridad a la hora de realizar las transacciones.

Estas mismas medidas sobre protección de usuarios tienen validez para todas las empresas españolas, pero también para aquellas integridad de dichos dispositivos.

3. Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores.

El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados.

Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado.

extranjerías que realicen envíos de carácter comercial a usuarios que residen en España.

Sin embargo, es más que probable que en los próximos años se siga trabajando para que tanto empresas como usuarios y trabajadores tengan las mayores garantías en torno al correo electrónico.

### **VALOR DOCUMENTAL DEL CORREO ELECTRÓNICO**

El correo electrónico es un medio de comunicación presente en nuestra vida cotidiana, y por supuesto también en la Administración pública. Eso ha tenido reflejo en la vida administrativa, que lo ha convertido en el vehículo de comunicación más usado. Tal circunstancia exige una estrategia clara y consideración adecuada, que arranca con la determinación de en qué casos el correo electrónico es un documento que debe ser tratado como tal.

La Ley 16/1985, de 25 de junio, del **Patrimonio Histórico Español**, define el **documento** en su artículo 49 como "*toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos*".

Por su parte, el glosario de términos del Esquema Nacional de Interoperabilidad (ENI)<sup>11</sup> define al **documento electrónico** como "*información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado*".

En línea con las características de **validez del documento electrónico** recogidas en el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (sustituida por la Ley 39/2015 de 1 de octubre), el artículo 26.2 del mencionado **ENI** define los requisitos para considerar válido

---

<sup>11</sup> Real Decreto 4/2010, de 8 de enero, por el que se regula el **Esquema Nacional de Interoperabilidad** en el ámbito de la Administración Electrónica.

## **DELEGADO PROTECCION DATOS. AYUNTAMIENTO ZARAGOZA**

---

un **documento electrónico** trasladado a un tercero por **medios electrónicos**:

- a) *"Contener información de cualquier naturaleza archivada en un soporte electrónico según un formato determinado susceptible de identificación y tratamiento diferenciado.*
- b) *Disponer de los datos de identificación que permitan su individualización, sin perjuicio de su posible incorporación a un expediente electrónico.*
- c) *Incorporar una referencia temporal del momento en que han sido emitidos.*
- d) *Incorporar los metadatos mínimos exigidos.*
- e) *Incorporar las firmas electrónicas que correspondan de acuerdo con lo previsto en la normativa aplicable."*

Nos acostumbramos a la cotidianidad alcanzada por el **correo electrónico**. También su aparente consideración como un medio informal de comunicación, con un uso de lenguaje menos formalizado que los clásicos escritos administrativos. Pero lo cierto es que, a la vista de estas definiciones, pocas dudas hay para considerar el **valor documental del correo electrónico**, entendido como **mensaje de comunicación**.

### **Hay correos-e que son prueba y son información**

El **valor documental** para las **administraciones públicas** de numerosos **correos electrónicos** viene determinada por el papel que juegan. Nos referimos a esos correos que, como los documentos, son una consecuencia de la actividad desarrollada por las instituciones. Y partiendo de esa actividad, la necesidad de **conservar determinados correos** va ligada estrechamente a su **valor probatorio** o a su valor histórico o cultural. Es decir, nos encontramos con correos electrónicos que son prueba y son información.

A título de muestra, veamos cinco argumentos suficientes, pero no exclusivos, que avalan **el valor documental de numerosos correos electrónicos.**

### **1.-Algunos correos-e han sustituido a documentos en papel**

El correo electrónico se ha extendido en la sociedad civil como una de las principales y más ágiles herramientas de comunicación. Esa misma realidad se ha impuesto en todas las administraciones públicas.

De esta manera, numerosas comunicaciones de papel han sido sustituidas por el **correo-e**. Una muy sencilla, que todo el mundo entenderá, es el conocido como "*de-a*"; es decir, "*De fulano a mengano*". De esta manera, una **remisión de documentación** que antes se hacía a través de **registro**, ahora es un simple **envío por correo electrónico**.

### **2.-Hay correos-e que forman parte de expedientes administrativos**

Los correos electrónicos pueden formar, y forman parte con frecuencia, de **trámites y procedimientos de los documentos** que integran algunos **expedientes**. La agilidad de este vehículo ha supuesto que numerosos **trámites internos** se sustituyan por correos, cuyo **borrado descontrolado** privaría al **expediente** de algunos de sus elementos. Pensemos, por ejemplo, en las continuas peticiones y envíos de informes sobre borradores y propuestas.

### **3.-Cada vez más los tribunales dan valor de prueba al correo-e**

El extendido uso del **correo electrónico** como medio de comunicación lo convierte en un potencial productor constante de pruebas. Es decir, el correo electrónico tiene una posible **trascendencia jurídica**. La consideración jurídica tiende a consagrar el hecho de que si no se prueba la falsedad, partimos de la premisa de su autenticidad. El **valor probatorio** que pueden alcanzar los correos electrónicos ante un **tribunal** deja pocas dudas con el caso **Urdangarín**.

## **DELEGADO PROTECCION DATOS. AYUNTAMIENTO ZARAGOZA**

---

En un litigio el correo electrónico se considera un **documento privado**, al que se le aplica el artículo 326 de la Ley de Enjuiciamiento Civil (LEC)<sup>12</sup>. Eso implica que si la parte que se pueda ver perjudicada por su contenido no impugna su autenticidad, será prueba en el proceso. Si lo impugna, lo valorará el juez. De ahí la existencia de empresas especializadas en la certificación y validación de la transmisión, el contenido y el acuse de recibo.

---

12 Artículo 326 LEC. **Fuerza probatoria de los documentos privados.**

1. Los documentos privados harán prueba plena en el proceso, en los términos del artículo 319, cuando su autenticidad no sea impugnada por la parte a quien perjudiquen.

2. Cuando se impugnare la autenticidad de un documento privado, el que lo haya presentado podrá pedir el cotejo pericial de letras o proponer cualquier otro medio de prueba que resulte útil y pertinente al efecto.

Si del cotejo o de otro medio de prueba se desprendiere la autenticidad del documento, se procederá conforme a lo previsto en el apartado tercero del artículo 320. Cuando no se pudiere deducir su autenticidad o no se hubiere propuesto prueba alguna, el tribunal lo valorará conforme a las reglas de la sana crítica.

3. Cuando la parte a quien interese la eficacia de un documento electrónico lo solicite o se impugne su autenticidad, integridad, precisión de fecha y hora u otras características del documento electrónico que un servicio electrónico de confianza no cualificado de los previstos en el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, permita acreditar, se procederá con arreglo a lo establecido en el apartado 2 del presente artículo y en el Reglamento (UE) n.º 910/2014.

4. Si se hubiera utilizado algún servicio de confianza cualificado de los previstos en el Reglamento citado en el apartado anterior, se presumirá que el documento reúne la característica cuestionada y que el servicio de confianza se ha prestado correctamente si figuraba, en el momento relevante a los efectos de la discrepancia, en la lista de confianza de prestadores y servicios cualificados.

Si aun así se impugnare el documento electrónico, la carga de realizar la comprobación corresponderá a quien haya presentado la impugnación. Si dichas comprobaciones obtienen un resultado negativo, serán las costas, gastos y

## **DELEGADO PROTECCION DATOS. AYUNTAMIENTO ZARAGOZA**

---

De acuerdo con el artículo 162 de dicha ley, para usar el correo electrónico como **prueba en juicio**, hay que adoptar las medidas adecuadas<sup>13</sup>.

Las empresas de **certificación electrónica** generan **actas de comunicación** que demuestran la transmisión, el contenido íntegro y el **acuse de recibo** de todos los correos electrónicos que hayan

---

derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación. Si, a juicio del tribunal, la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 300 a 1200 euros.

13 Artículo 162 LEC **Actos de comunicación por medios electrónicos, informáticos y similares.**

1.-Cuando las oficinas judiciales y las partes o los destinatarios de los actos de comunicación estén obligados a enviarlos y recibirlos **por medios electrónicos**, telemáticos, infotelecomunicaciones o de otra clase semejante, que permitan el envío y la recepción de escritos y documentos, de forma tal que esté garantizada la autenticidad de la comunicación y de su contenido y quede constancia fehaciente de la remisión y recepción íntegras y del momento en que se hicieron, o cuando los destinatarios opten por estos medios, los actos de comunicación se efectuarán por aquellos, con el resguardo acreditativo de su recepción que proceda.

Los profesionales y destinatarios obligados a utilizar estos medios, así como los que opten por los mismos, deberán comunicar a las oficinas judiciales el hecho de disponer de los medios antes indicados y la dirección electrónica habilitada a tal efecto.

Asimismo se constituirá en el Ministerio de Justicia un registro accesible electrónicamente de los medios indicados y las direcciones correspondientes a los organismos públicos y profesionales obligados a su utilización.

2.-En cualquiera de los supuestos a los que se refiere este artículo, cuando constando la correcta remisión del acto de comunicación por dichos medios técnicos, salvo los practicados a través de los servicios de notificaciones organizados por los Colegios de Procuradores, transcurrieran tres días sin que el destinatario acceda a su contenido, se entenderá que la comunicación ha sido efectuada legalmente desplegando plenamente sus efectos.

Se exceptuarán aquellos supuestos en los que el destinatario justifique la falta de acceso al sistema de notificaciones durante ese periodo. Si la falta de acceso se

validado. El **Tribunal Supremo** ya ha avalado en autos este planteamiento.

### **4.-La ley 39/2015 acepta el correo-e como "aviso de notificación"**

La **Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas**, cita el correo electrónico como una opción de "**avisos de notificación**" en sus relaciones con los ciudadanos.

Ese aviso de notificación de "*puesta a disposición*" también lo contempla en el artículo 152 la [Ley de Enjuiciamiento Civil](#)<sup>14</sup>, si bien ésta también lo incluye en el mismo artículo como una de las formas válidas para los "*actos de comunicación*", así como uno de los datos debiera a causas técnicas y éstas persistiesen en el momento de ponerlas en conocimiento, el acto de comunicación se practicará mediante entrega de copia de la resolución. En cualquier caso, la notificación se entenderá válidamente recibida en el momento en que conste la posibilidad de acceso al sistema. No obstante, caso de producirse el acceso transcurrido dicho plazo pero antes de efectuada la comunicación mediante entrega, se entenderá válidamente realizada la comunicación en la fecha que conste en el resguardo acreditativo de su recepción.

14 Artículo 152 LEC. **Forma de los actos de comunicación. Respuesta.**

1. Los actos de comunicación se realizarán bajo la dirección del letrado de la Administración de Justicia, que será el responsable de la adecuada organización del servicio. Tales actos se ejecutarán por:

1.º Los funcionarios del Cuerpo de Auxilio Judicial.

2.º El procurador de la parte que lo solicite.

A tal efecto, en todo escrito que dé inicio a un procedimiento judicial, de ejecución, o a otra instancia, el solicitante deberá expresar si interesa que todos los actos de comunicación se realicen por su procurador. Si no se manifestare nada al respecto, el letrado de la Administración de Justicia dará curso a los autos, realizándose tales actos por los funcionarios del Cuerpo de Auxilio Judicial. Asimismo, serán realizados por estos últimos si los demandados, ejecutados o recurridos no solicitan expresamente en su escrito de personación que se realicen por su procurador o si las partes fueran beneficiarias del derecho de asistencia jurídica gratuita.

que el **demandante** puede aportar sobre el **demandado** (artículo 155), como "*instrumento de comunicación*" con la oficina judicial (artículo 155).

### **5. -La ley 40/2015 incluye el correo-e entre las reuniones por vías electrónicas**

La ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, reconoce la posibilidad de celebrar y convocar **reuniones**

Los solicitantes podrán, de forma motivada y concurriendo justa causa, pedir la modificación del régimen inicial, procediendo el letrado de la Administración de Justicia, si lo considera justificado, a realizar los sucesivos actos de comunicación conforme a la nueva petición.

Se tendrán por válidamente realizados estos actos de comunicación cuando en la diligencia quede constancia suficiente de haber sido practicados en la persona, en el domicilio, en la dirección electrónica habilitada al efecto, por comparecencia electrónica o por los medios telemáticos o electrónicos elegidos por el destinatario.

A estos efectos, el procurador acreditará, bajo su responsabilidad, la identidad y condición del receptor del acto de comunicación, cuidando de que en la copia quede constancia fehaciente de la recepción, de su fecha y hora y del contenido de lo comunicado.

2. Los actos de comunicación se practicarán por medios electrónicos cuando los sujetos intervinientes en un proceso estén obligados al empleo de los sistemas telemáticos o electrónicos existentes en la Administración de Justicia conforme al artículo 273, o cuando aquéllos, sin estar obligados, opten por el uso de esos medios, con sujeción, en todo caso, a las disposiciones contenidas en la normativa reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

No obstante, los actos de comunicación no se practicarán por medios electrónicos cuando el acto vaya acompañado de elementos que no sean susceptibles de conversión en formato electrónico o así lo disponga la ley.

El destinatario podrá identificar un dispositivo electrónico, servicio de mensajería simple o una dirección de correo electrónico que servirán para informarle de la puesta a su disposición de un acto de comunicación, pero no para la práctica de notificaciones. En tal caso, con independencia de la forma en que se realice el acto de comunicación, la oficina judicial enviará el referido aviso. La falta de práctica de este aviso no impedirá que la notificación sea considerada

de **órganos colegiados y conferencias sectoriales por medios electrónicos**, entre ellos el correo electrónico, siempre que esos medios, entre otros requisitos, "*garanticen la intercomunicación entre ellos y la unidad de acto*".

### **Una estrategia para el correo-e**

Es evidente, por tanto, que en determinados casos, **los correos electrónicos adquieren la categoría de documento electrónico**. Eso exige abordarlo en tal consideración, algo que pocas veces sucede. Uno de esos escasos lugares es la *Política de gestión de documentos electrónicos MINHAP (PGDE)*, que dedica un apartado a esta interesante cuestión, tratada también de forma monográfica en el anexo de *Ponencias* de dicha PGDE.

En este sentido, resulta interesante recoger aquí la estrategia marcada en el **MINHAP** para asegurar la **conservación a largo plazo de los correos electrónicos** que la organización decida conservar, **garantizando la accesibilidad, confidencialidad, integridad y disponibilidad**:

- *Definirá qué mensajes deberán ser conservados a largo plazo*
- *Establecerá distinciones entre correos personales, oficiales a conservar a largo plazo y resto de correos oficiales*
- *Establecerá el tratamiento a aplicar a cada uno de estos grupos*
- *Determinará el valor de los correos desde el momento de su creación o recepción e indicará los metadatos necesarios para asegurar su conservación y su contextualización*
- *Fijará los sistemas de firma electrónica y cifrado de datos necesarios para asegurar su integridad y autenticidad*

La estrategia deberá aplicarse en el momento de la **creación o recepción de los correos electrónicos**.

## DELEGADO PROTECCION DATOS. AYUNTAMIENTO ZARAGOZA

---

Es importante tener en cuenta lo dispuesto en el **Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos**, al amparo de la Ley 39/2015, de 1 de octubre, y la Ley 40/2015, de 1 de octubre, para llevar a cabo su desarrollo reglamentario en lo referido a la gestión electrónica de los procedimientos y el funcionamiento electrónico del sector público

A continuación incorporamos al texto información de utilidad facilitada por **Redes y Sistemas**:

Esta información aunque pueda estar un poco obsoleta (en cuanto a tamaños de buzón, de mensajes, etc, esos datos habría que revisarlos) tiene algunos datos interesantes:

- "cuenta de correo personalizada bajo el dominio "@zaragoza.es" para todo el personal municipal": es decir, cuando una persona pierde la condición de personal municipal, ya no tiene derecho a la cuenta de correo corporativa.
- "instrumentos que permitan al personal municipal el acceso a los medios que ofrece la Sociedad de la Información", "intercambio de mensajes con direcciones de correo electrónico ajenas al Ayuntamiento de Zaragoza": quiere decir que la cuenta de correo electrónico no está limitada al uso interno, sino que se puede utilizar con otros usos y comunicarnos con entidades ajenas al Ayuntamiento. Por tanto, técnicamente no se puede limitar que una persona use esta cuenta de correo para fines particulares (uso de redes sociales, dar esta dirección para el banco, etc.)

**Cómo se dan de baja las cuentas de correo**: cuando desde Recursos Humanos llega a Redes y Sistemas una baja (jubilación, cese, excedencia...) a los 3 meses:

- se borra el buzón de correo de esa persona, se eliminan todos los mensajes
- se inhabilita el usuario de correo y se guarda en un histórico

## **DELEGADO PROTECCION DATOS. AYUNTAMIENTO ZARAGOZA**

---

Las cuentas de correo no se reutilizan: por ejemplo, si cuando yo causo baja y se incorpora un trabajador con mi misma inicial de nombre y mismo apellido, en ningún caso se le asignará mmarco, sino que se usará su segundo apellido para crearle la cuenta de correo (ejemplo mmarcog)

### **Correo Personal.**

La antigua **Delegación de Ciencia y Tecnología** promovió en su día una actuación para dotar de los instrumentos que permitan al personal municipal el acceso a los medios que ofrece la Sociedad de la Información. Para ello, se van a proporcionar los siguientes servicios:

- Navegación por Internet desde todos los puestos de trabajo municipales.
- Cuenta de correo personalizada bajo el dominio "@zaragoza.es" para todo el personal municipal.

### **Cómo usar la cuenta de correo personalizada**

Desde cualquier ordenador con acceso a Internet:

Puede utilizar su cuenta de correo personal desde cualquier sitio con acceso a Internet, conectándose a la página <http://webmail.zaragoza.es> e introduciendo su nombre de usuario y contraseña. Esta contraseña coincide con la de su correo electrónico interno (que es la misma que la de la entrada en la red).

### **Dudas o incidencias:**

Para resolver cualquier problema relativo al acceso a través de Internet, dispone de un servicio de atención exclusivo e independiente para resolución de dudas o incidencias:

Por Teléfono: su teléfono habitual de Asistencia a Usuarios de Informática, de lunes a viernes de 10 a 12 horas,

### **Desde su puesto de trabajo:**

Si en su puesto de trabajo emplea un programa cliente de correo (Netscape Messenger, Mozilla Thunderbird o Microsoft Outlook Express), puede configurarlo para usar su nueva cuenta de correo personal, para lo cual debe seguir los pasos detallados en la página: <http://intranet.red.zaragoza.es/correopersonal/instrucciones/>.

### **Diferencia entre las cuentas de correo personal y las cuentas de correo interno:**

Estas nuevas cuentas de correo personal sustituyen a las actuales cuentas de correo interno, que sin embargo podrán seguir siendo utilizadas en lo sucesivo. Todos los mensajes enviados a la cuenta de correo personal de un usuario podrán ser leídos por medio de su correspondiente cuenta interna y viceversa. En ningún caso se pierden correos ni de la cuenta personal ni de la interna. La única diferencia entre ambos tipos de cuenta es que con la personal es posible el intercambio de mensajes con direcciones de correo electrónico ajenas al Ayuntamiento de Zaragoza, cosa que no se permite con la cuenta interna.

### **Cómo conocer la dirección de correo electrónico personal de un usuario.**

- **Guía de direcciones**

Existe una guía de direcciones global que se puede consultar tras conectarse a <http://webmail.zaragoza.es> utilizando un nombre de usuario y contraseña válidos. Por medio de ella es posible localizar la dirección de correo electrónico de cualquier empleado municipal a partir de su nombre o primer apellido.

- **Herramienta de búsqueda de la intranet.** Introduzca un criterio de búsqueda (nombre y/o apellidos), para localizar la dirección de correo electrónico de cualquier empleado municipal.

### Normas de uso:

- No se admite ninguna solicitud de cambio de nombre de cuenta de correo. Su generación ha sido automática a partir de la inicial del nombre y el primer apellido, usando la inicial del segundo apellido para resolver las coincidencias entre varias personas.
- El tamaño de los buzones de correo electrónico es de 50 MB.
- Restricciones que se aplican a los mensajes intercambiados con cuentas de correo electrónico ajenas al Ayuntamiento de Zaragoza:
  - Tamaño máximo de mensaje de 5 MB.
  - 5 ficheros adjuntos como máximo.
  - No se permiten ficheros adjuntos de vídeo, música, etc.

### Servicio de Correo Electrónico Multidominio

#### Descripción

El **correo electrónico multidominio** permite desde un punto centralizado, dar servicio de correo electrónico y agenda electrónica sin necesidad de tener instalaciones in situ o contrataciones externas. Incluye correo electrónico sobre clientes pesados (Outlook, Thunderbird, etc...), correo web, correo sobre dispositivos móviles, sincronización de agendas, listas de distribución, etc. Al mismo tiempo permite la gestión descentralizada de los buzones de cada dominio por parte de los Organismos adheridos

El correo electrónico es uno de los servicios más demandados en la actualidad como sistema de información y comunicaciones. El crecimiento en su uso ha sido exponencial en los últimos años y hoy resulta imprescindible. Pero como toda infraestructura de tecnologías de la información conlleva unos costes.

Con la **solución de correo multidominio** se consigue:

- Reducción de costes de operación y mantenimiento para los Organismos adheridos al presentarse el correo como un servicio.

- Mantener unas políticas de servicio de correo electrónico homogéneas para todos los Organismos adheridos.

A continuación analizamos como ilustración **una sentencia** de la **AN** reciente, sobre el uso inadecuado del correo electrónico en un ayuntamiento:

### **¿Puede usarse el correo electrónico almacenado en un fichero de atención al ciudadano para fomentar la participación ciudadana en un Ayuntamiento?**

La Sala de lo Contencioso-Administrativo de la Audiencia Nacional ha dictado sentencia el 22 de febrero de 2019, confirmando la resolución dictada por la Agencia Española de Protección de Datos (AEPD) que había declarado la comisión de una infracción grave por parte del Ayuntamiento de Madrid, por haber vulnerado el principio de calidad de datos de la ya derogada LOPD (artículo 4 apartados 1 y 2).

El citado Ayuntamiento había utilizado las **direcciones de correo electrónico de varios vecinos**, que se habían almacenado en el fichero “Servicios de Atención al Ciudadano” para informar de la apertura de un nuevo sitio web (Decide Madrid), cuya finalidad es que los ciudadanos, previo registro, envíen ideas para mejorar la ciudad de Madrid.

De hecho, y según se desprende de esta sentencia, se habían enviado un total de 223.000 correos electrónicos.

Entre las alegaciones que realiza ese Ayuntamiento destaca la referente a que el tratamiento del dato del correo electrónico no es incompatible con la finalidad que motivó su recogida originaria, ya que *“encaja plenamente en las competencias municipales. Se invoca el artículo 4 del Reglamento Orgánico de Participación Ciudadana del Ayuntamiento de Madrid de 31 de mayo de 2004”*.

De esta forma, *“Se acordó utilizar el dato de la cuenta de correo electrónico de aquellos usuarios que constaba en el sistema CRM, que da cobertura técnica al tratamiento de datos del fichero “Servicios de Atención al Ciudadano” con el objeto de enviarles*

## **DELEGADO PROTECCION DATOS. AYUNTAMIENTO ZARAGOZA**

---

*información por el Delegado del Área de Gobierno de Participación Ciudadana, Transparencia y Gobierno Abierto. Y en este sentido, en el correo que se remitió, como ha quedado anteriormente reseñado, se indica que se ha utilizado para realizar el envío del correo la dirección de correo electrónico que consta en el fichero "Atención al Ciudadano".*

Sobre si este uso es compatible o no con la finalidad que recabó su recogida inicial, en la sentencia se indica lo siguiente:

*Y esto es lo que ha acontecido en el caso que nos ocupa, ya que la finalidad del fichero al que se incorporaron los correos electrónicos de los ciudadanos, era para facilitar la gestión de contactos con los ciudadanos, que unido al servicio "Línea Madrid" , hay que referirlos la gestión concreta que los ciudadanos pretendían realizar en algún servicio del Ayuntamiento.*

*Ello no ampara, como pretende la parte recurrente, que se encuentre incluido en el consentimiento de los ciudadanos para la utilización de su correo electrónico para recibir el correo en cuestión, siendo una finalidad distinta que hubiese requerido un consentimiento al efecto.*

*La finalidad de la información de la existencia de una plataforma para dar ideas a fin de mejorar la ciudad, no puede quedar comprendida, dentro del consentimiento dado para el fichero de donde se obtuvieron las direcciones de correo electrónico, que era para facilitar la gestión de contacto con el ciudadano. Por otro lado, el art. 69.1 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local , prevé que " Las Corporaciones locales facilitaran la más amplia información sobre su actividad y la participación de todos los ciudadanos en la vida local", y una cosa, es la información sobre la participación de los ciudadanos en la vida local, y otra, como se deriva de los correos enviados, una información sobre la existencia de una plataforma para exponer ideas para mejorar la ciudad, que rebasa para la finalidad para las que el dato de carácter personal, como es la dirección de correo electrónico.*

## **DELEGADO PROTECCION DATOS. AYUNTAMIENTO ZARAGOZA**

---

*Muestra de ello, que dicho dato se recoge de un solo fichero, como es el "Atención al Ciudadano", y no de otros, habiéndose necesitado para ello un acuerdo de 3 de agosto de 2015 entre la Dirección General de Calidad y Atención al Ciudadano, responsable del servicio "Línea Madrid", y la Dirección General de Participación Ciudadana.*

*Igualmente, tampoco ampara la no necesidad de consentimiento para el envío del correo electrónico en cuestión, el art. 4 del Reglamento Orgánico de Participación Ciudadana del Ayuntamiento de Madrid de 31 de mayo de 2004 , por las mismas razones antes expuestas, y sobre todo, en relación con el segundo denunciante, que no está empadronado en Madrid, ya que no resultaría aplicable, pues el mismo hace referencia a los ciudadanos de Madrid, y así el párrafo primero establece: " El Ayuntamiento de Madrid garantizará a los ciudadanos del municipio su derecho a la información sobre la gestión de las competencias y servicios municipales, de acuerdo con las disposiciones legales vigentes y la presente normativa, con los únicos límites previstos en el artículo 105, párrafo b), de la Constitución ".*

Por otra parte, y aunque los hechos ocurrieron antes de que el RGPD fuese ya de aplicación (mayo de 2018), destacar que la última parte de la sentencia se dedica a incidir sobre **la regulación del consentimiento en la norma europea**, transcribiendo los considerandos 32, 39, 43 y 50, así como también transcribir el artículo 6 de la LOPD-GDD, para terminar con la siguiente **conclusión** al respecto:

*Por lo que en virtud de lo expuesto, cuando el tratamiento tenga varios fines, debe darse **el consentimiento para todos ellos**, y los fines específicos del tratamiento de los datos personales deben ser **explícitos y legítimos**, y deben determinarse en el momento de su recogida, y con el objeto de determinar si el fin del tratamiento ulterior es compatible con el fin de la recogida inicial de los datos personales, el responsable del tratamiento, debe tener en cuenta,*

## **DELEGADO PROTECCION DATOS. AYUNTAMIENTO ZARAGOZA**

---

*entre otras cosas, cualquier relación entre los fines del tratamiento original y los fines del tratamiento ulterior previsto, el contexto en el que se recogieron los datos, en particular las expectativas razonables del interesado basadas en su relación con el responsable en cuanto a su uso posterior.*

I. C. Zaragoza 18 de enero de 2022.