POLÍTICA INTERNA DE PROTECCIÓN DE DATOS EN MAS BUSINESS

DICIEMBRE 2020

Política interna de protección de datos de **MAS Business** para responder a la ley de Reglamento General de Protección de Datos (GDPR).

En **MAS Business** cuidamos por seguir y cumplir la ley de GDPR en todos los ámbitos de la empresa en el que se recojan y usen datos de personas físicas.

Por ello hemos creado esta política interna que se separa en los siguientes apéndices:

1. Principales cambios en la ley de protección de datos que nos afecta
2. Datos tratados por **MAS Business**
3. Obtención de los datos
4. Medidas de seguridad aplicadas
5. Medidas técnicas
6. Formación de personal

Principales cambios en la ley de protección de datos que nos afecta

Esta nueva ley incluye nuevos ámbitos que afectan a nuestro tratamiento de datos de nuestros clientes, potenciales clientes, proveedores y empleados.

Los nuevos cambios que nos afectan son:

1. Se refuerzan las garantías para que el interesado vea salvaguardado su derecho y pueda hacerlo valer ante quien trata sus datos. Se establece un marco mucho más desarrollado de figuras tales como el consentimiento que debe ser explícito e inequívoco y, también en el momento de recoger los datos, habrá de informarse de la base legal y de los intereses legítimos del responsable sobre los que se desarrolla el tratamiento de datos. Todo esto obligará a revisar y modificar las políticas de protección de datos de las organizaciones responsables del tratamiento de datos de carácter personal.

2. Se añaden nuevos derechos a los ya conocidos derechos A.R.C.O. (acceso, rectificación, cancelación y oposición):
   a. El derecho al olvido (derecho al borrado de los datos personales).
   b. El derecho de limitación de tratamiento. (Una finalidad no excluirá el derecho del tratamiento para los interesados. Por ejemplo, en nuestras webs pueden o no aceptar las dos finalidades impuestas para el uso de sus datos)
   c. El derecho de portabilidad (el derecho a la portabilidad implica que los datos personales del interesado se puedan y deban transmitirse directamente de un responsable a otro, sin necesidad de que sean transmitidos previamente al interesado).

3. Se prevén medidas de responsabilidad activa de los responsables:
   a. Se deberá realizar una valoración y análisis del riesgo de los tratamientos que se realicen y que deberá documentarse.
   b. Se deberá establecer una política interna de protección de datos, que deberá ser conocida por todos los trabajadores debiendo probarse dicho conocimiento.
   c. Instauración de políticas de obtención y tratamiento de los mínimos datos posible.

Datos tratados por MAS Business

En **MAS Business** tratamos datos personales considerados de bajo riesgo. Se consideran datos de bajo riesgo cuando no se tratan de datos sensibles. Los datos que regula este reglamento son los datos que tenemos en los siguientes soportes:

- Zoho
- Mailchimp
- Personal (Datos de nosotros y cuentas bancarias)
- Proveedores (Solo entrarían nuestros proveedores autónomos)

La mayoría de los datos tratados por nosotros se pueden clasificar de bajo riesgo al usar datos comunes de personas físicas como:

- Nombre y apellidos
- Correo electrónico
- Teléfono
- Dirección postal

En algunos casos y excepcionalmente se utilizan datos sensibles de proveedores o personal de la empresa como pueden ser:

- Cuentas bancarias
- Datos profesionales
- Datos académicos

Para estos datos solo la dirección de **MAS Business** tiene acceso a estos datos y deberán extremar al máximo las medidas de seguridad que se establecen en este documento y en las píldoras formativas.

Obtención de los datos

Los datos obtenidos por MAS Business han sido captados de forma lícita a través de los siguientes canales:

- **A través de formularios web en las páginas de**: **MAS Business**, **LBG** y **ONLBG**. Estas páginas cuentan con sus políticas de privacidad adaptadas a la nueva ley para la obtención del consentimiento explícito e inequívoco del uso de datos personales sus datos para las finalidades estipuladas en las políticas.
- **A través de tarjetas de contactos entregados por las personas.** Tarjetas de contacto que recibimos de las personas en eventos o reuniones.
- **A través de correos directos a cualquiera de los correos de empresa de MAS Business.** En nuestras firmas se establecen las condiciones del tratamiento de datos.

Ningún dato ha sido captado de forma ilícita y sin el consentimiento expreso de su propietario. Si se detectase algún dato que no lleva el consentimiento explícito de la persona física este dato se eliminará inmediatamente de nuestra base de datos.

Para evitar la obtención de datos no necesarios para nuestra prestación de servicios nos hemos asegurado de no pedir datos que no son necesarios.
Por ello tenemos separado los datos según su finalidad:

1. **Datos obtenidos de páginas webs, tarjetas de visita, clientes y proveedores:** Estos datos se utilizará para proveer el servicio contratado o para contactar con posibles clientes. Si el usuario ha dado su consentimiento se podrá utilizar para enviar comunicaciones comerciales exclusivas de MAS Business.

2. **Personal y proveedores autónomos**: Estos datos serán utilizados solo para la gestión de nóminas del equipo de **MAS Business.**

Medidas de seguridad aplicadas

Las medidas de seguridad aplicadas variaran según el nivel de riesgo de los datos tratados.

Por ello diferenciaremos las medidas de seguridad por las tres áreas detectadas de tratamiento de datos:

1. **Datos obtenidos de páginas webs, tarjetas de visita, clientes y proveedores:** Estos datos se encontrarán almacenados en la aplicación online de ZOHO. Cada miembro de la empresa cuenta con sus propios accesos para así conseguir una trazabilidad de los datos usados. Zoho será la encargada del tratamiento de los datos al usar sus servidores como repositorio de nuestros datos.

2. **Personal y proveedores autónomos**: Estos datos se encontrarán almacenados de forma cifrada en los ordenadores centrales de **MAS Business** con copias de seguridad y que solo tendrá acceso los máximos responsables de la empresa para la gestión de las nóminas y de las facturas.

Para asegurar una correcta seguridad de los datos **MAS Business** ha puesto en conocimiento a todo su personal de sus obligaciones para establecer los requisitos de seguridad en el tratamiento de datos personal.

Todo el personal con acceso a los datos personales deberá tener conocimiento de sus obligaciones con relación a los tratamientos de datos personales y serán informados acerca de dichas obligaciones. La información mínima que será conocida por todo el personal será la siguiente:

1. **Deber de confidencialidad y secreto**
   a. Se deberá evitar el acceso de personas no autorizadas a los datos personales, a tal fin se evitará: dejar los datos personales expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público, soportes con datos personales, etc.).
   Cuando se ausente del puesto de trabajo, se procederá al bloqueo de la pantalla o al cierre de la sesión.
   b. Los documentos en papel y soportes electrónicos se almacenarán en lugar seguro (armarios o estancias de acceso restringido) durante las 24 horas del día.
   c. No se desecharán documentos o soportes electrónicos (cd, pen drives, discos duros, etc.) con datos personales sin garantizar su destrucción.
   d. No se comunicarán datos personales o cualquier información personal a terceros, se prestará atención especial en no divulgar datos personales protegidos durante las consultas telefónicas, correos electrónicos, etc.
   e. El deber de secreto y confidencialidad persiste incluso cuando finalice la relación laboral del trabajador con la empresa.

2. Derechos de los titulares de los datos

Se informará a todos los trabajadores acerca del procedimiento para atender los derechos de los interesados, definiendo de forma clara los mecanismos por los que pueden ejercerse los derechos (medios electrónicos, referencia al Delegado de Protección de Datos si lo hubiera, dirección postal, etc.) teniendo en cuenta lo siguiente:

a. Previa presentación de su documento nacional de identidad o pasaporte, los titulares de los datos personales (interesados) podrán ejercer sus derechos de acceso, rectificación, supresión, oposición y portabilidad. El responsable del tratamiento deberá dar respuesta a los interesados sin dilación indebida.
b. Para el **derecho de acceso** se facilitará a los interesados la lista de los datos personales de que disponga junto con la finalidad para la que han sido recogidos, la identidad de los destinatarios de los datos, los plazos de conservación, y la identidad del responsable ante el que pueden solicitar la rectificación supresión y oposición al tratamiento de los datos.
c. Para el **derecho de rectificación** se procederá a modificar los datos de los interesados que fueran inexactos o incompletos atendiendo a los fines del tratamiento.
d. Para el **derecho de supresión** se suprimirán los datos de los interesados cuando los interesados manifiesten su negativa u oposición al consentimiento para el tratamiento de sus datos y no exista deber legal que lo impida.
e. Para el **derecho de portabilidad** los interesados deberán comunicar su decisión e informar al responsable, en su caso, sobre la identidad del nuevo responsable al que facilitar sus datos personales.

El responsable del tratamiento deberá informar a todas las personas con acceso a los datos personales acerca de los términos de cumplimiento para atender los derechos de los interesados, la forma y el procedimiento en que se atenderán dichos derechos.

3. Violaciones de seguridad de datos de carácter personal

Cuando se produzcan violaciones de seguridad DE DATOS DE CARÁCTER PERSONAL, como, por ejemplo, el robo o acceso indebido a los datos personales se notificará a la Agencia Española de Protección de Datos en término de 72 horas acerca de dichas violaciones de seguridad, incluyendo toda la información necesaria para el esclarecimiento de los hechos que hubieran dado lugar al acceso indebido a los datos personales. La notificación se realizará por medios electrónicos a través de la sede electrónica de la Agencia Española de Protección de Datos en la dirección: https://sedeagpd.gob.es

Medidas técnicas

1. Identificación

a. Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador.
b. Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.
c. Se garantizará la existencia de contraseñas para el acceso a los datos personales almacenados en sistemas electrónicos. La contraseña tendrá al menos 8 caracteres, mezcla de números y letras.
d. Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos personales, se dispondrá de un usuario y contraseña específicos (identificación inequívoca).
e. Se debe garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. Para la gestión de las contraseñas puede consultar la guía de privacidad y seguridad en internet de la Agencia Española de Protección de Datos y el Instituto Nacional de Ciberseguridad. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y el acceso de personas distintas del usuario.

2. Deber de salvaguarda

A continuación, se exponen las medidas técnicas mínimas para garantizar la salvaguarda de los datos personales:

a. ACTUALIZACIÓN DE ORDENADORES Y DISPOSITIVOS: Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la media posible.
b. MALWARE: En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema de antivirus que garantice en la medida posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.
c. CORTAFUEGOS O FIREWALL: Para evitar accesos remotos indebidos a los datos personales se velará para garantizar la existencia de un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales.
d. CIFRADO DE DATOS: Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá valorar la posibilidad de utilizar un

método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.

e. COPIA DE SEGURIDAD: Periódicamente se realizará una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar seguro, distinto de aquél en que esté ubicado el ordenador con los ficheros originales, con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información.

Las medidas de seguridad serán revisadas de forma periódica, la revisión podrá realizarse por mecanismos automáticos (software o programas informáticos) o de forma manual. Considere que cualquier incidente de seguridad informática que le haya ocurrido a cualquier conocido le puede ocurrir a usted, y prevéngase contra el mismo.

Formación del personal

Para asegurarnos el correcto seguimiento de las normas de seguridad comentadas anteriormente se realizarán píldoras de formación periódicas seguidos de una valoración de conocimientos. Se realizará 4 formaciones desde junio a septiembre para tratar los temas de:

1. La información
2. Soportes
3. El puesto de trabajo
4. Dispositivos móviles

Estas formaciones conllevarán una evaluación cada una y se irán ampliando semestralmente para así asegurar el correcto entendimiento por parte de nuestro personal de estas nuevas medidas.

Firmado:

John Charlton Scade
Director General / Responsable de tratamiento