COMUNICADO COLABORADORES/AS: PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

I. Recogida y tratamiento de datos personales

T-Systems ITC Iberia, S.A.U. (en lo sucesivo, T-Systems) garantiza a sus colaboradores/as que la recogida y el tratamiento de sus datos de carácter personal se realiza siempre 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 (en lo sucesivo, RGPD) y en las Binding Corporate Rules Privacy (en lo sucesivo, BCRP) que recogen los requisitos para el tratamiento de datos personales así como los derechos de los interesados dentro del grupo Deutsche Telekom AG.

Así, T-Systems asegura que la información facilitada por los colaboradores/as recibe un tratamiento absolutamente confidencial y no se utiliza ni se divulga con fines distintos a los que justifican su registro.

Los datos de carácter personal de los colaboradores/as de T-Systems (incluida su imagen) se incluyen en tratamientos titularidad de T-Systems con la finalidad de:

- Facilitar la gestión de los recursos necesarios para la confección de ofertas y ejecución de proyectos concretos (datos de CV).
- Publicarlos en el directorio de la intranet de T-Systems a efectos de facilitar el contacto y la localización entre los empleados/as, así como, por motivos de seguridad, en las tarjetas de acceso a las instalaciones.
- Incluirlos en tratamientos para la gestión de las infraestructuras, videovigilancia o sistemas de soporte a los procesos de negocio de T-Systems.

Adicionalmente, T-Systems realiza aquellas cesiones de los datos personales de los colaboradores/as que son pertinentes y estrictamente necesarias a las administraciones públicas o entidades privadas, con el objetivo de presentarse a un concurso o de presentar una oferta.

El/La titular de los datos tiene los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad de los datos y oposición que podrá ejercitar bajo los términos y condiciones de los arts. 15 y siguientes del RGPD. Para ello, se deberá contactar con T-Systems por correo en la dirección c/ Pere IV 313-321, 08020 Barcelona o por correo electrónico en la dirección fmb.ts-ib-protec-datos-personales@t-systems.com.

II. Acceso y tratamiento de datos personales

Todos los colaboradores/as de T-Systems que en el desarrollo de sus funciones tengan la necesidad de acceder a las instalaciones o a la información contenida en tratamientos de titularidad de T-Systems o de terceros, tienen la obligación de seguir y respetar las directrices descritas a continuación.

a) Confidencialidad

El colaborador/a tratará con estricta confidencialidad cualquier tipo de información o datos que se le proporcionen para el desarrollo de sus funciones, teniendo en cuenta que esa información/datos son propiedad de T-Systems o de sus clientes y que poseen un valor comercial.

El colaborador/a garantiza que los datos o información a los que tiene acceso no se utilizarán para usos o finalidades distintos a los que motivan su comunicación.

Este compromiso de confidencialidad se mantendrá aun cuando hubiese finalizado la colaboración.

b) Tratamiento de datos de carácter personal

El colaborador/a está obligado a velar por el adecuado cumplimiento del RGPD, de las BCRP (Section 4), así como de cualquiera otra disposición vigente o que en el futuro se apruebe sobre datos de carácter personal.

[Sección 4 BCRP:
§ 22 Calidad de los datos
(1) Los datos personales serán correctos y, en su caso, se mantendrán actualizados (exactitud de los datos).
(2) Teniendo en cuenta la finalidad para la que se tratan los datos, se tomarán las medidas adecuadas para garantizar que se elimine, bloquee o, si es necesario, corrija cualquier información incorrecta o incompleta.

§ 23 Seguridad de los datos – medidas técnicas y organizativas – protección de datos desde el diseño y por defecto
La empresa adoptará las medidas técnicas y organizativas adecuadas para los procesos, los sistemas informáticos y las plataformas de la empresa utilizados para recopilar, procesar o emplear datos con el fin de proteger estos datos, que se evalúan periódicamente en cuanto a su eficacia.
Dichas medidas incluirán:
a) impedir que personas no autorizadas accedan a los sistemas de tratamiento de datos en los que se procesan o utilizan los datos personales (control de acceso);
b) garantizar que los sistemas de procesamiento de datos no puedan ser utilizados por personas no autorizadas (control de denegación de uso);
c) garantizar que las personas autorizadas a utilizar un sistema de tratamiento de datos puedan acceder exclusivamente a los datos a los que han autorizado el acceso (control de acceso a los datos) y que los datos personales no puedan ser leídos, copiados, alterados o eliminados durante el tratamiento por personas no autorizadas (por ejemplo, mediante cifrado);
d) garantizar que, en el curso de la transmisión electrónica o durante su transporte o grabación en soportes de datos, los datos personales no puedan ser leídos, copiados, alterados o eliminados por personas no autorizadas, y que sea posible comprobar e identificar a los responsables a los que se transmitirán los datos personales mediante equipos de transmisión de datos (control de transmisión de datos);
e) garantizar que sea posible examinar y establecer retrospectivamente si los datos personales han sido introducidos en los sistemas de tratamiento de datos, modificados o eliminados y por quién (control de entrada de datos);
f) garantizar que los datos personales subcontratados solo puedan procesarse de acuerdo con las instrucciones del cliente (control del procesador);
g) garantizar que los datos personales estén protegidos contra la destrucción o pérdida accidental (control de disponibilidad);
h) garantizar que los datos que se hayan recopilado para diferentes fines puedan tratarse por separado (norma de separación).
Si el colaborador/a detecta una anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal de un cliente o de T-Systems, deberá informar a su responsable y notificarlo al buzón de protección de datos (fmb.ts-ib-protec-datos-personales@t-systems.com).]

Adicionalmente, cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de titularidad de T-Systems se notificará al buzón de seguridad corporativa (fmb.ts-ib-security-management@t-systems.com).

En la notificación se indicará el tipo de incidencia (con descripción detallada), cómo se ha detectado, la fecha y hora en que se ha producido y los efectos que ha producidos o que pudieran producirse.

c) Consecuencias del incumplimiento

El incumplimiento de la obligación de confidencialidad por parte del colaborador/a se podrá considerar como incumplimiento grave y doloso del contrato correspondiente y podrá constituir causa de terminación contractual; todo ello sin perjuicio de la sanción administrativa que pudiera corresponder.

☐ Como colaborador/a de T-Systems acepto que he leído este comunicado y en prueba de conformidad lo firmo en fecha _____.