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 comunicaciones 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 (Sección 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 _____.

NOTICE TO CONTRIBUTORS: PROTECTION OF PERSONAL DATA

I. Collection and processing of personal data

T-Systems ITC Iberia, S.A.U. (hereinafter, T-Systems) guarantees to its contributors that the collection and processing of their personal data is performed in accordance with the provisions of Regulation (EU) 2016/679, of April 27 2016, on the protection of natural persons with regard to the of personal data and on the free movement of such data (hereinafter, RGPD) and the Binding Corporate Rules Privacy (hereinafter, BCRP) that include the requirements for the processing of the personal data as well as the processing of the rights of the interested parties at the Deutsche Telekom AG group.

Thus, T-Systems guarantees that the information provided by the contributors is treated strictly as confidential and is not used or disclosed for other purposes than those justified in their registry.

The personal data of the contributors of T-Systems (including their image) are included in files owned by T-Systems with the following purpose:

- Facilitate the management of the resources needed for the preparation of tenders and the execution of certain projects (CV's data).
- Release the data within the directory included in the intranet of T-Systems to facilitate the contact and location between the employees and, for security reasons, in the card to access the premises.
- Include them in the files for the management of infrastructures, video surveillance or support systems for the business processes of T-Systems.

Additionally, T-Systems performs those assignments of personal data of the contributors that are relevant and strictly necessary to the public administrations or the private entities with the aim of appearing before a tender o submitting an offer.

The holder of the data has the rights of access, rectification, erasure, restriction of processing, data portability and the right to object that may be executed under the terms and conditions set out in articles 15 and following of the RGPD. To this purpose, is required to contact T-Systems by post at the address c/ Pere IV 313-321, 08020, Barcelona or by e-mail at the address: fmb.ts-ib-protec-datos-personales@t-systems.com.

II. Access and processing of personal data

All the contributors of T-Systems that in the development of their functions need to have access to the premises or the information included within the files owned by T-Systems or third parties, are obliged to follow and respect the directions described below.

a) Confidentiality

The contributor shall treat any information or data that has been provided to him/her for the development of his/her functions in strict confidence, considering that said information/data are owned by T-Systems or its clients and have a commercial value.

The contributor ensures that the information/data which are accessible to him/her shall not be used for any purposes other than those who motivate the communication.

The confidentiality compromise shall continue to apply even though the contribution has ended.

b) Treatment of personal data

The contributor shall ensure the proper compliance of the RGPD, the BCRP (Section 4) as well as the compliance with any other legislation in force or that may be approved in the future regarding personal data.

[Section 4 BCRP:

§ 22 Data quality

(1) Personal data shall be correct and, where necessary, kept up to date (data accuracy).

(2) In light of the purpose for which the data is being processed, appropriate measures shall be taken to ensure that any incorrect or incomplete information is erased, blocked or, if necessary, corrected.

§ 23 Data security – technical and organisational measures – data protection by design and default

The company shall take appropriate technical and organisational measures for company processes, IT systems and platforms used to collect, process or employ data in order to protect this data, which are evaluated on a regular basis regarding their effectiveness.

Such measures shall include:

a) preventing unauthorized persons from gaining access to data processing systems on which personal data is processed or used (admittance control);

b) ensuring that data processing systems cannot be used by unauthorized persons (denial-of-use control);

c) ensuring that those persons authorized to use a data processing system are able to access exclusively the data to which they have authorized access (data access control) and that personal data cannot, during processing be read, copied, altered or removed by unauthorized persons (e.g. by encryption);

d) ensuring that, in the course of electronic transmission or during its transport or recording on data media, personal data cannot be read, copied, altered or removed by unauthorized persons, and that it is possible to check and identify the controllers to which personal data is to be transmitted by data transmission equipment (data transmission control);

e) ensuring that it is possible retrospectively to examine and establish whether and by whom personal data has been entered into data processing systems, altered or removed (data entry control);

f) ensuring that outsourced personal data can only be processed in accordance with the instructions of the customer (processor control);

g) ensuring that personal data is protected against accidental destruction or loss (availability control);

h) ensuring that data which has been collected for different purposes can be processed separately (separation rule)].

In the event the contributor is aware of an anomaly that affects or may affect the safety of the personal data of a client or T-Systems, he/she shall report it to his/her manager and to the mailbox of data protection (fmb.ts-ib-protec-datos-personales@t-systems.com).

Additionally, any anomaly that affects or may affect the safety of the data owned by T-Systems shall be notified to the mailbox of corporate security (fmb.ts-ib-security-management@t-systems.com).

The notification shall include the type of incident (with a detailed description), how it was detected, date and time of the incident and effects.

c) Consequences of non-compliance

Failure to comply with the obligation of confidentiality by the contributors may be understood as a very serious infraction and willful infringement of the corresponding agreement and may be considered as a cause for its termination; all the abovementioned without prejudice of the administrative sanction that may correspond.

☐ As contributor of T-Systems I declare that I have read the present document and proving its acceptance I sign it on the date _____.

COMUNICAT COL·LABORADORS I COL·LABORADORES: PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

I. Recollida i tractament de dades personals

T-Systems ITC Iberia, S.A.U. (en endavant, T-Systems) garanteix als seus col·laboradors i col·laboradores que la recollida i el tractament de les seves dades de caràcter personal es realitza sempre de conformitat amb l'establert al Reglament (UE) 2016/679, de 27 d'abril, relatiu a la protecció de les persones físiques en el que respecta al tractament de dades personals i a la lliure circulació d'aquestes dades (en endavant, RGPD) i amb les Binding Corporate Rules Privacy (en endavant, BCRP) que recullen els requisits per al tractament de dades personals així com els drets dels interessats i les interessades dins el grup Deutsche Telekom AG.

D'aquesta forma, T-Systems assegura que la informació facilitada pels col·laboradors i col·laboradores rep un tractament absolutament confidencial i no és utilitzada ni divulgada amb finalitats diferents a aquella que va justificar el seu registre

Les dades de caràcter personal dels col·laboradors i col·laboradores de T-Systems (inclosa la seva imatge) s´inclouen en tractaments titularitat de T-Systems amb la finalitat de:

- Facilitar la gestió dels recursos necessaris per a la confecció d'ofertes i l'execució de projectes concrets (dades de CV).
- Publicar-les en el directori de la intranet de T-Systems a efectes de facilitar el contacte i la localització entre els empleats i empleades, així com, por motius de seguretat, en les targes d'accés a les instal·lacions.
- Incloure-les en tractaments per a la gestió de les infraestructures, video-vigilància o sistemes de suport als processos de negoci de T-Systems.

Addicionalment T-Systems realitza les comunicacions de les dades personals dels col·laboradors i col·laboradores que resulten pertinents i estrictament necessàries a les administracions públiques o entitats privades amb l'objectiu de presentar-se a un concurs o de presentar una oferta.

El/al titular de les dades té els drets d'accés, rectificació, supressió, limitació del tractament, portabilitat de les dades i oposició, que podrà exercitar sota els termes i condicions contemplats en els articles 15 i següents del RGPD. Per això, s'haurà de contactar amb T-Systems per correu a l'adreça c/ Pere IV 313-321, 08020 Barcelona o per correu electrònic a l'adreça fmb.ts-ib-protec-datos-personales@t-systems.com.

II. Accés i tractament de dades personals

Tots els col·laboradors i col·laboradores de T-Systems que en el desenvolupament de les seves funcions tinguin la necessitat d'accedir a les instal·lacions o a la informació continguda en fitxers de titularitat de T-Systems o de tercers, tenen l'obligació de seguir i respectar les directrius descrites a continuació.

a) Confidencialitat

El col·laborador/a tractarà amb estricta confidencialitat qualsevol tipus d'informació o dades que li siguin proporcionats per al desenvolupament de les seves funcions, tenint en compte que aquella informació/dades són propietat de T-Systems o dels seus clients i posseeixen un valor comercial.

El col·laborador/a garanteix que la informació/dades a que té accés no seran utilitzades per a usos o finalitats diferents a les que motiven la seva comunicació.

Aquest compromís de confidencialitat continuarà vigent encara que hagués finalitzat la col·laboració.

b) Tractament de dades de caràcter personal

El col·laborador/a està obligat a vetllar per l'adequat compliment del RGPD, de les BCRP (Secció 4) així com de qualsevol altre disposició vigent o que en el futur s'aprovi sobre sobre dades de caràcter personal.

[Secció 4

§ 22 Qualitat de les dades

1) Les dades personals han de ser correctes i, si escau, estar actualitzades (exactitud de les dades).
2) Tenint en compte la finalitat per a la qual s'estan tractant les dades, s'adoptaran les mesures oportunes per garantir que qualsevol informació incorrecta o incompleta sigui esborrada, bloquejada o, si escau, corregida.

§ 23 Seguretat de les dades: mesures tècniques i organitzatives: protecció de dades per disseny i predeterminat. L'empresa ha d'adoptar les mesures tècniques i organitzatives adequades per als processos de l'empresa, sistemes informàtics i plataformes utilitzats per recopilar, processar o utilitzar dades per protegir aquestes dades, que s'avaluen periòdicament pel que fa a la seva eficàcia.

Aquestes mesures inclouran:

a. impedir que persones no autoritzades accedeixin als sistemes de tractament de dades en què es tracten o utilitzen dades personals (control d'admissió);
b. garantir que els sistemes de tractament de dades no puguin ser utilitzats per persones no autoritzades (control de denegació d'ús);
c. garantir que les persones autoritzades per utilitzar un sistema de tractament de dades puguin accedir exclusivament a les dades a les quals tenen accés autoritzat (control d'accés a les dades) i que les dades personals no puguin, durant el tractament, ser llegits, copiats, alterats o eliminats per persones no autoritzades (per exemple, mitjançant xifratge);
d. vetllar perquè, en el curs de la transmissió electrònica o durant el seu transport o enregistrament en suport de dades, les dades personals no puguin ser llegits, copiats, alterats o suprimits per persones no autoritzades, i que sigui possible comprovar i identificar els responsables del tractament als quals s'han de transmetre les dades personals mitjançant equips de transmissió de dades (control de transmissió de dades);
e. vetllar per que sigui possible examinar i establir de manera retroactiva si i per qui s'han introduït dades personals en sistemes de tractament de dades, alterades o eliminades (control d'entrada de dades);
f. garantir que les dades personals subcontractades només es puguin tractar d'acord amb les instruccions del client (control de l'encarregat);
g. garantir que les dades personals estiguin protegides contra la destrucció o la pèrdua accidentals (control de disponibilitat);
h. garantir que les dades recollides per a diferents finalitats es puguin tractar per separat (regla de separació)].

Si el col·laborador/a detecta una anomalia que afecti o pugui afectar a la seguretat de les dades de caràcter personal d'un client o de T-Systems haurà d'informar al seu responsable i notificar-ho a bústia de protecció de dades fmb.ts-ib-protec-datos-personales@t-systems.com.

Addicionalment, qualsevol anomalia que afecti o pugui afectar a la seguretat de les dades de titularitat de T-Systems es notificarà a la bústia de seguretat corporativa (fmb.ts-ib-security-management@t-systems.com).

A la notificació s'indicarà el tipus d'incidència (descripció detallada), com s'ha detectat, la data i l'hora en que s'ha produït i els efectes que s'han produït o que es poguessin produir.

c) Conseqüències de l'incompliment

L'incompliment de l'obligació de confidencialitat per part del col·laborador/a es podrà considerar com incompliment greu i dolós del contracte corresponen i podrà constituir causa de terminació contractual; tot això sense perjudici de la sanció administrativa que pogués correspondre.

☐ Com col·laborador/a declaro que he llegit aquest document i en prova de conformitat el signo a data _____