



# Information des collaborateurs La protection des données

Brochure sur la protection des données pour les collaboratrices et collaborateurs conformément au RGPD



C'EST QUOI ... LA PROTECTION DES DONNÉES ?



## Chère collègue, cher collègue !

La question de la protection des données vous concerne, à un double point de vue. D'une part en tant que client ou collaborateur dont les données sont traitées et, d'autre part, parce que, lors de votre activité, vos données à caractère personnel peuvent être portées à la connaissance de tiers. Le droit de la protection des données ne vous autorise à traiter les données à caractère personnel de collaborateurs, clients, fournisseurs ou autres tiers uniquement dans le cadre des prescriptions légales et conformément aux instructions internes correspondantes. Préserver la confidentialité est une obligation sur le plan du droit du travail et sur celui de la protection des données.

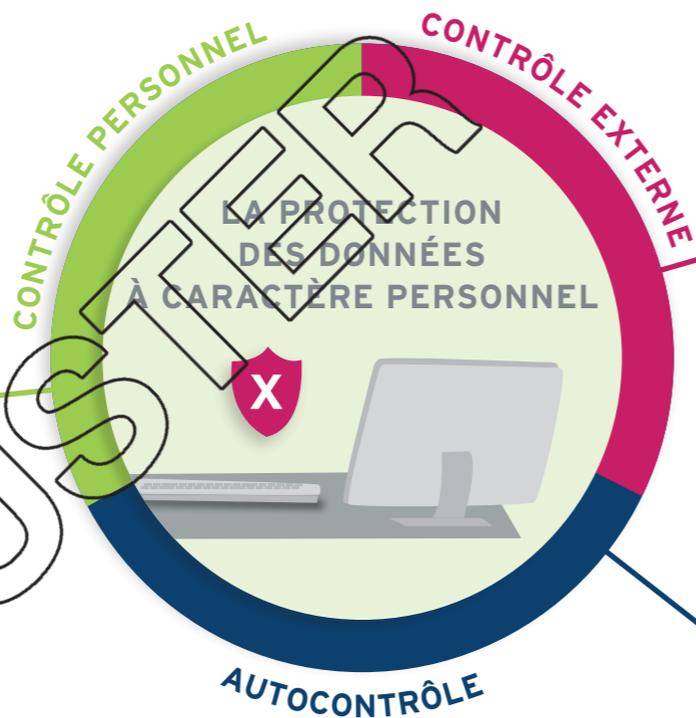
La base juridique en est le Règlement général sur la protection des données (RGPD). Il a pour objectif de moderniser et uniformiser la protection des données dans l'UE. De plus, le RGDP autorise les États membres de l'UE à adopter des dispositions spécifiques relatives à des thèmes déterminés.

Le but de la protection des données, à savoir à protéger l'individu contre toute atteinte à son droit de la personnalité dans le contexte de l'utilisation de ses données à caractère personnel, exige une action dans un esprit de responsabilité lors de l'exploitation des données à caractère personnel, mais aussi un rapport conscient vis-à-vis des risques pour les systèmes et applications d'informatique.

Cette brochure d'information des collaborateurs se propose de vous donner un aperçu sur les fondamentaux de la protection des données et de vous informer au sujet de vos droits et de vos devoirs. Dans ma fonction de responsable de la protection des données, je me tiens bien évidemment à votre entière disposition au cas où vous auriez des doutes ou des questions. N'hésitez pas à vous adresser à moi, en toute confiance.

*Votre responsable de la protection des données*

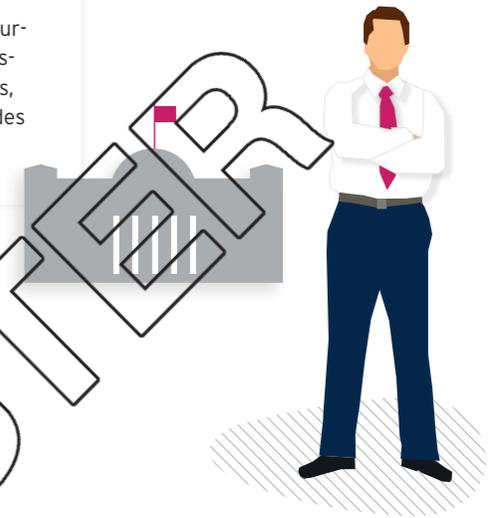
# LA PROTECTION DES DONNÉES D'UN SEUL COUP D'ŒIL



**La personne concernée**  
 ... exerce ses droits  
 Elle peut demander des renseignements au sujet de données sauvegardées et, le cas échéant, exiger que ces données soient rectifiées, effacées, bloquées ou transférées.  
 » À PARTIR DE LA PAGE 16



**L'État**  
 ... contrôle le respect  
 L'instance de régulation pour la surveillance des données peut contester des procédures non autorisées, infliger des amendes et déposer des plaintes pénales.  
 » À PARTIR DE LA PAGE 6



**L'entreprise**  
 ... assume la responsabilité de ce que le traitement des données à caractère personnel ne s'effectue que conformément au droit de la protection des données.  
 » À PARTIR DE LA PAGE 8

... organise la protection des données  
 L'entreprise énonce les critères pour la méthode et les conditions du prélèvement et du traitement des données à caractère personnel.  
 » À PARTIR DE LA PAGE 12

... sécurise les données  
 Les données à caractère personnel doivent être suffisamment protégées contre tout accès non autorisé, contre la perte et la destruction.  
 » À PARTIR DE LA PAGE 14











# TOUTE L'ENTREPRISE EST RESPONSABLE !



**DIRECTION**  
Elle assume la responsabilité de la protection des données en interne et en externe



**CADRE SUPERIEUR**



**LE RESPONSABLE DE LA PROTECTION DES DONNEES**  
Le responsable de la protection des données conseille la direction, les membres du personnel et les personnes concernées au sujet de la protection des données, dont il contrôle le respect.



**COLLABORATEUR**  
Il protège les données à caractère personnel contre tout accès non autorisé et toute transmission non autorisée.

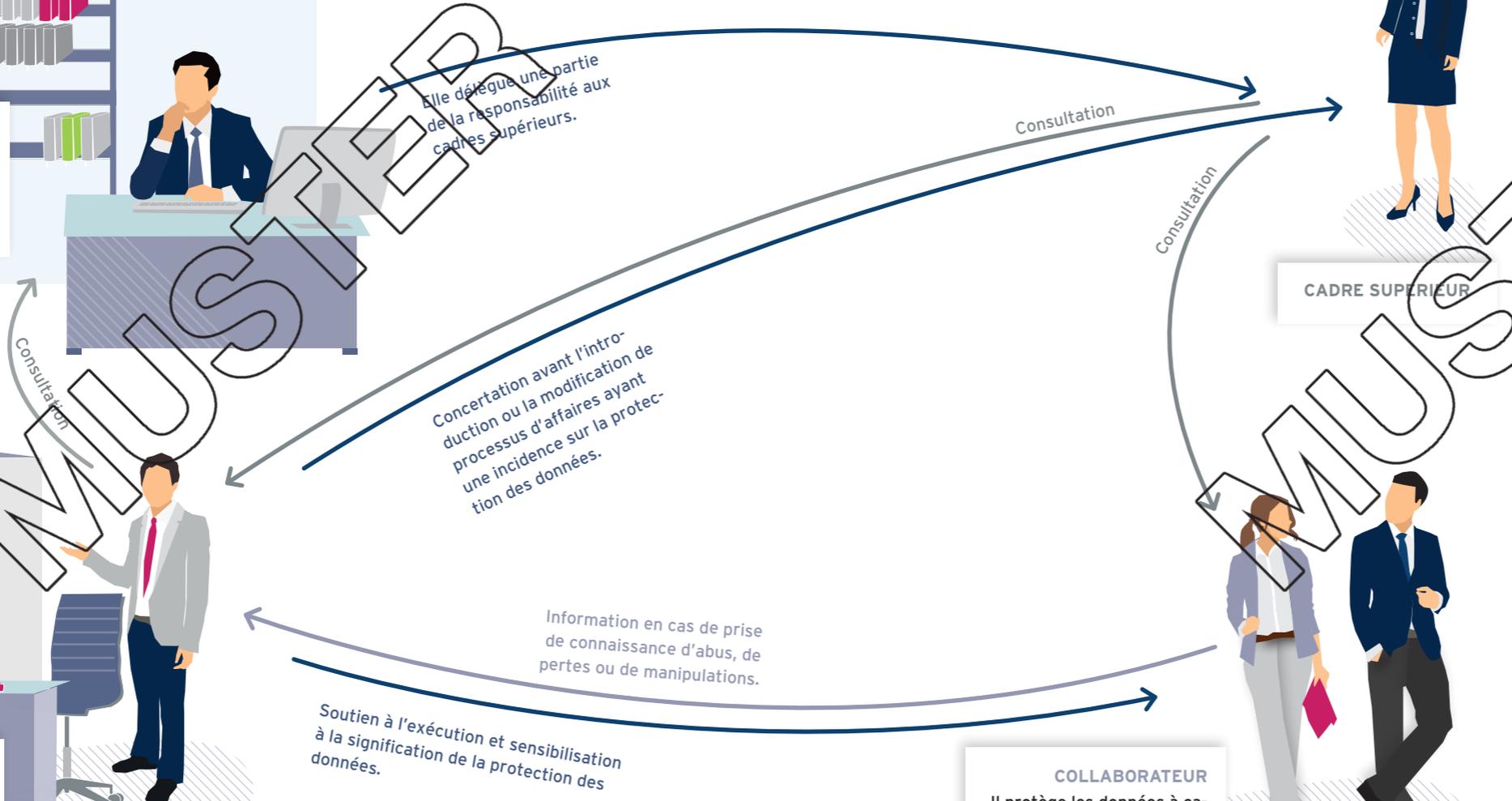


## La protection des données comme mission des services spécialisés et des collaborateurs

Les cadres supérieurs et les collaborateurs assument une lourde responsabilité quant à la mise en œuvre du RGPD. Ils doivent veiller aux processus de conformité avec la protection des données : le traitement des données doit être licite et les droits des personnes concernées doivent pouvoir être respectés. C'est le service technique compétent qui est responsable de la documentation dans le répertoire des activités de traitement.

En cas de traitement de données critiques, il est impératif de procéder à une estimation des conséquences de la protection des données, lors de laquelle le responsable de la protection de données au sein de l'entreprise doit être consulté.

**EN CAS DE QUESTIONS**  
sur le thème de la protection des données et de la sécurité de données, ou en cas de doute, veuillez vous adresser au ou à la responsable de la protection des données au sein de votre entreprise.



# LES OBJECTIFS DE SÉCURITÉ POUR LA SÉCURITÉ DES DONNÉES

## DATAKONTEXT DATAKONTEXT DAT

**§ Art. 32 RGPD**  
Le responsable du traitement est tenu de définir les risques inhérents au traitement et de prendre des mesures pour les réprimer. Les suivants doivent être atteints :

Pour garantir la sécurité et prévenir toute infraction à la protection des données, l'entreprise est tenue de définir les risques inhérents au traitement et de prendre des mesures pour les réprimer.

Les suivants doivent être atteints :

- La pseudonymisation et le chiffrement de données à caractère personnel
- La capacité à garantir durablement la confidentialité, l'intégrité, la disponibilité et la robustesse de systèmes et services dans le contexte du traitement
- La capacité à restaurer rapidement la disponibilité de données à caractère personnel et l'accès à celles-ci en cas d'incident physique ou technique
- Une procédure de vérification, qui permet l'évaluation à intervalle régulier de l'efficacité des mesures techniques et organisationnelles permettant de garantir la sécurité du traitement.

### 1. Confidentialité

#### ■ Contrôle d'entrée

Pas d'utilisation non autorisée des installations de traitement de données, par exemple : cartes magnétiques ou à puce, clés, gachets électroniques, gardiennage interne ou conciergerie, alarmes, installations vidéos.

#### ■ Contrôle des accès aux bâtiments

Pas d'utilisation non autorisée de systèmes, par exemple : mots de passe (sûrs) nécessaires le clicke au biométriques, authentification à deux facteurs, chiffrement de support de données.

#### ■ Contrôle d'accès

Pas de consultation, copiage, modification ou enlèvement sans autorisation au sein du système, par exemple : concepts d'habitation et droits d'accès, en fonction des besoins, enregistrement des accès.

#### ■ Contrôle de l'itération

Traitement séparé de données qui ont été prélevées à des fins différentes, par exemple multi-localisation sécurisée.

#### ■ Pseudonymisation

Le traitement de données à caractère personnel d'une manière telle que, sans devoir recourir à des informations supplémentaires, les données ne puissent plus être affectées à une personne concernée de façon spécifique dans la mesure où les informations supplémentaires ont été conservées séparément et sont associées à des mesures techniques et organisationnelles correspondantes.

## DATAKONTEXT DATAKONTEXT DAT

### 2. Intégrité

#### ■ Contrôle de la transmission

Pas de consultation, copiage, modification ou enlèvement sans autorisation lors du transfert électronique ou du transport, par exemple : chiffrement, Virtual Private Networks (VPN), signature électronique.

#### ■ Contrôle de la saisie

Constatation et purge des données à caractère personnel non créées, supprimées ou enlevées dans des systèmes de traitement de données, par exemple : enregistrement des notes, gestion des documents.

### 3. Disponibilité et robustesse

#### ■ Contrôle de la disponibilité

Protection contre toute destruction et/ou perte fortuite ou malveillante, par exemple : stratégie de backup (on-line/hors-ligne, on-site/hors-site), alimentation en courant sans interruption (ASI), protection antivirus, pare-feu, transmission des informations et plan de secours.

#### ■ Restaurabilité rapide

### 4. Procédure de vérification récurrente, planification et évaluation

#### ■ Gestion de la protection des données

#### ■ Incident - Response Management

#### ■ Paramétrage facilitant la protection des données (article 25, annexe 2, RGPD)

#### ■ Contrôle des ordres

Pas de traitement de données sur ordre sans instruction correspondante du donneur d'ordre, par exemple : rédaction sans ambiguïté du contrat, gestion des ordres formalisés, sélection rigoureuse du prestataire de services, obligation de conviction préliminaire, contrôles ultérieurs.

#### ■ Article 25 - DP

Il exige la protection des données par la configuration de la technique (privacy by design) et par des paramètres favorisant la protection de données (privacy by default)

# LES DROITS DE LA PERSONNE CONCERNÉE

Le RGPD désigne « personne concernée » la personne physique dont les données sont traitées et dont les droits de personnalité méritent d'être protégés aux termes de la loi. Les personnes concernées peuvent être le collaborateur, le client ou l'interlocuteur auprès d'une société cliente. Le délai accordé des droits de transparence et d'intervention aux personnes concernées.

## DROITS D'INTERVENTION

La personne concernée a le droit de savoir à quelles fins ses données sont traitées et quels sont ses droits en matière de protection des données. Ceci déclenche des obligations de transparence auprès de l'entreprise.



### ATTENTION

La personne concernée a le droit de s'adresser au responsable de la protection des données de l'entreprise en cas de plaintes ou de demandes relatives à la personne concernée. Celui-ci est soumis à l'obligation de confidentialité dès lors que cette personne ne l'en a pas exonéré.

#### Rectification

Seules des données pertinentes ont le droit d'être traitées. Sinon, il convient de les rectifier.

#### Effacement

Les données doivent être effacées après leur usage prévu ou à l'arrivée à expiration de prescriptions de conservation.

#### Droit à l'oubli

Si l'entreprise a publié des données devant obligatoirement être effacées, l'entreprise est tenue, à la demande de la personne concernée, de rechercher qui a des liens avec ces données ou les a adaptées. Ces tiers doivent être informés au sujet de l'exigence d'effacement.

#### Opposition

Pour des motifs inhérents à sa situation particulière, la personne concernée peut faire opposition au traitement des données lorsque la licéité de ce traitement repose sur une pondération des intérêts. La personne concernée peut aussi faire opposition à la publicité directe.

#### Transmission de données

Si la personne concernée a mis des données à disposition, par exemple sur un réseau social ou dans un compte de clients, ces données doivent être transmises par le responsable à la personne concernée dans un format courant et structuré lisible à la machine ou à un autre responsable.

#### Restriction du traitement

Lorsque l'exactitude des données est contestée par des personnes concernées ou lorsque la personne concernée a besoin de données pour sa défense juridique en cas d'obligations d'effacement, celles-ci devraient être bloquées. Cela vaut même titre pour les obligations légales de conservation par l'entreprise.

PERSONNE CONCERNÉE





## CONSEILS PRATIQUES SUR LA PROTECTION DES DONNÉES

Chaque collaborateur assume une part de responsabilité envers la protection des données au sein de l'entreprise. Aussi et surtout dans son propre intérêt, une de ses tâches consiste à respecter les règles de protection des données dans son entreprise et à assumer ses tâches en tenant compte de la protection des données.

Conseils simples pour la protection des données ayant cependant une validité générale :

### **Clean desk**

Un bureau bien rangé, le principe clean desk, garantit la sécurité de données et leur confidentialité. Les données à caractère personnel et les secrets de l'entreprise doivent être protégés pour ne pas tomber aux mains de personnes non autorisées. En cas d'absence, les dossiers, clés USB, supports de données, etc. doivent être rangés dans un endroit fermé à clé.

### **Renseignement donné au téléphone**

Les demandes de renseignements à caractère personnel, aussi bien en interne qu'en externe, doivent faire l'objet d'un examen critique sous l'angle de la protection des données. En cas de demande de renseignements par téléphone, en particulier, il convient de faire preuve de circonspection quant à la personne appelant et au contenu de la conversation et, en cas de doute, lui recommander la voix écrite.

### **Séparation d'un système**

Toujours séparer le système avant de quitter son poste de travail.

### **Protection visuelle de l'écran**

Positionner l'écran de manière à le protéger des regards curieux émanant de collègues, visiteurs ou clients. En voyage, il convient d'utiliser un filtre de confidentialité.

### **Transmission sécurisée de courriels**

Lorsque l'on a l'intention de transmettre en toute sécurité des courriels confidentiels, il convient de les crypter. Renseignez-vous auprès de votre responsable de la sécurité de l'IT ou de la protection des données au sujet des protocoles de chiffement appropriés.

### **Ouverture de courriels**

Dans leur grande majorité, les virus informatiques se propagent par le biais des pièces jointes aux courriels. Celles-ci contiennent des programmes malveillants, tels que des virus, des chevaux de Troie ou de vers informatiques. En cas d'échec de votre protection antivirus, nous vous recommandons, en présence de courriels suspects, de toujours vous assurer, par un appel, que l'annexe a réellement été envoyée par la personne ou l'institution mentionnée comme expéditeur.

### **REMARQUE :**

Protéger ses données signifie protéger ses collègues et les clients et se protéger soi-même !

### Informations bibliographiques émanant de la Deutsche Bibliothek

La Deutsche Bibliothek enregistre la présente publication dans la Deutsche Nationalbibliographie; vous trouverez des données bibliographiques détaillées sur Internet en cliquant sur <http://dnb.ddb.de>.

Information des collaborateurs La protection des données -  
Brochure sur la protection des données pour les collaboratrices et collaborateurs conformément au RGPD

ISBN 978-3-89577-817-9

GDD - Gesellschaft für Datenschutz und Datensicherheit e.V.  
28<sup>ème</sup> édition revue et actualisée 2018

© 2018 DATAKONTEXT GmbH, Frechen  
[www.datakontext.com](http://www.datakontext.com)

la présente œuvre, y compris la totalité de ces éléments, est protégé par les droits d'auteur. Toute utilisation non prévue dans le strict cadre de la loi sur le droit d'auteur est, sans l'autorisation de la maison d'édition, illicite et susceptible de poursuites pénales. Cela vaut en particulier pour les duplications, les traductions, les microfilms, ainsi que le stockage et le traitement dans des systèmes électroniques. Un octroi de licence est possible après accord.

**Éditeur :** Gesellschaft für Datenschutz und Datensicherheit e.V., Bonn

**Maquette et composition :** Esther Gonstalla, Erdgeschoss Grafik, Hamburg

**Illustration :** Line Wittemann, Ârtisserie, Münster

**Crédit iconographique (Cover) :** contrastwerkstatt © [www.fotolia.de](http://www.fotolia.de)

Printed in Germany

Des prix dégressifs sont proposés pour la présente brochure.

Informations sous : 02234/98949-26

Remarque : pour des motifs de lisibilité, il a été renoncé à la succession de désignations de genre au masculin ou au féminin et, au lieu de cela, seule une forme a été utilisée. Bien évidemment, toutes les déclarations se dessinent au même titre aux collaboratrices et aux collaborateurs.

MUSTER



Gesellschaft für Datenschutz  
und Datensicherheit e.V.

