



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.

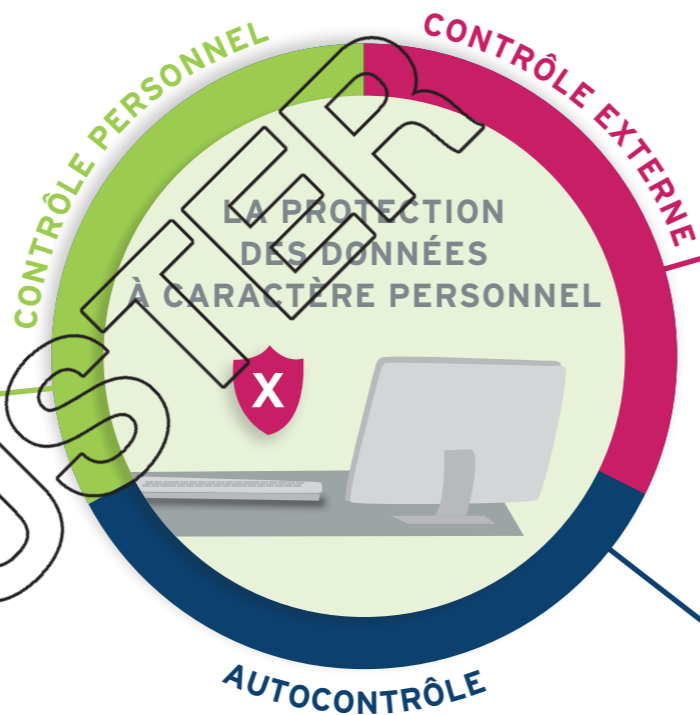
La base juridique en est le Règlement général sur la protection des données (RGPD). Il a pour objectif de moderniser et uniformiser la protection des données dans l'UE. De plus, le RGDP autorise les États membres de l'UE à adopter des dispositions spécifiques relatives à des thèmes déterminés.

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

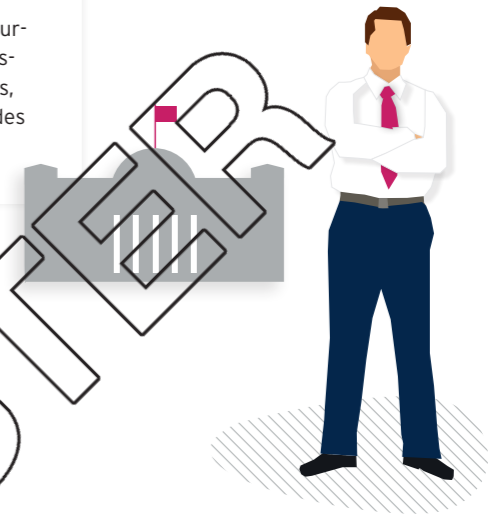
LA PROTECTION DES DONNÉES D'UN SEUL COUP D'ŒIL



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

LA SIGNIFICATION DE LA PROTECTION DES DONNÉES

Pourquoi la protection des données est-elle nécessaire ?

Le développement technologique du traitement automatisé de données entraîne une recrudescence des dangers d'utilisation abusive des données. De plus en plus de données sont produites, lesquelles peuvent être sauvegardées, combinées et exploitées de façon pratiquement illimitée. De ce fait, l'individu subit une atteinte à ses droits à sa personnalité et à sa liberté, en particulier quand il ne sait pas qui détient des données à son sujet ni lesquelles, ni ce que le détenteur en fait et à qui il les retransmet.

Qu'entend-on par données à caractère personnel ?

Les données à caractère personnel sont des indications relatives à une personne physique déterminée ou déterminable.

Exemples	PATRIMOINE	COMPORTEMENT AU TRAVAIL	IDENTIFIANT
ADRESSE	POSSESSION	NUMÉRO PERSONNEL	TEMPS D'UTILISATION D'UNE MACHINE DÉTERMINÉE
DATE DE NAISSANCE	SALAIRE	RÉSULTATS DU TRAVAIL	
NUMÉRO DE TÉLÉPHONE	PHOTO		

Des données particulièrement sensibles sont, par exemple, l'origine raciale et ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'affiliation à un syndicat, la santé et la vie sexuelle ainsi que les données biométriques et génétiques. Le traitement n'est autorisé que selon des règles strictes, leur utilisation étant, en règle générale, illicite, par exemple à des fins de marketing.

Quelles sont les bases juridiques ?

En raison des dangers pour le droit de la personnalité, tout traitement de données à caractère personnel requiert une base juridique. Les bases de la protection des données sont régies à l'échelle européenne par Règlement général sur la protection des données (RGPD). Il existe en outre des prescriptions spécifiques à des domaines déterminés. (voir page 9)

§ Art. 1 alinéa 2 RGPD
« Le présent règlement protège les droits fondamentaux et les libertés fondamentales des personnes physiques et, en particulier, leur droit à la protection des données à caractère personnel. »

i Art. 4 n° 1 RGPD
« Par données à caractère personnel, on entend toutes les informations qui se réfèrent à une personne physique identifiée ou identifiable ; par identifiant, on entend une personne physique que l'on peut identifier, directement ou indirectement, en particulier à l'aide de l'affectation à une désignation comme un nom, un numéro d'identification, des données de sites. »

! MAXIME
Chaque collaborateur doit gérer les données à caractère personnel avec minutie et prudence ! (Voir page 7/8)

Qui est protégé par le Règlement général sur la protection des données (RGPD) ?

Que les personnes le sèrent en leur sur la protection de données protégé le RGPD protège les personnes physiques lors de l'utilisation de leurs données à caractère personnel. Sont par conséquent protégés les collaborateurs, les clients et fournisseurs ou leurs intermédiaires. (voir page 10) Le des de protection de données dépend du contexte de leur utilisation.

QUI DOIT RESPECTER LE RGPD ?

- 1. Les organisations de droit privé de la société, mais aussi les personnes qui traitent des données à caractère personnel, par exemple, les indépendants, les associations, les entreprises industrielles, commerciales et tertiaires, mais aussi les prestataires de réseaux sociaux.**
- 2. Toutes les autres organisations de droit privé dont le but commercial est le traitement de données à caractère personnel pour les tiers, comme les centres de calcul de services, les organismes de renseignements économiques, les analystes de marché et les sondeurs d'opinion, les revendeurs, cour les et maisons d'édition d'adresses ainsi que les organismes de recherche scientifique et les médias.**
- 3. Les services publics et les autorités**

LES FORMES DE MANIEMENT DES DONNÉES À CARACTÈRE PERSONNEL

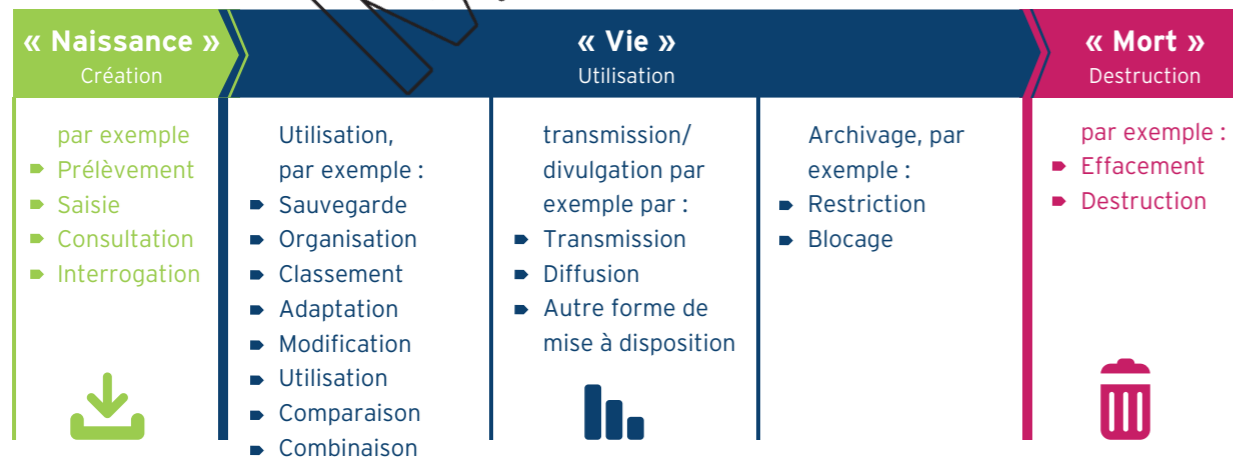
Le RGPD s'applique au traitement automatisé de données à caractère personnel ainsi qu'au traitement automatisé de données à caractère personnel dans un système de fichiers (par exemple fiches).

La notion de traitement dans l'esprit du RGPD s'applique au processus de manie- ment des données à caractère personnel. Le traitement commence avec l'obten- tion des données auprès de la personne concernée (par exemple sur interrogation écrite ou orale) ou auprès de tiers (par exemple achat d'adresses auprès de reven- deurs d'adresses) et, en passant par leur utilisation (par exemple l'exploitation ou la transmission, va jusqu'à leur occultation.

REMARQUE
Tout traitement de données doit s'effectuer en confor- mité avec le RGPD ou une autre prescription juridique ou avec le consentement de la personne concernée.

MUSSELER

DATA-LIFE-CYCLE



EXEMPLES : LICITE OU NON ?

- Une entreprise sauvegarde ses données clients pour l'exécution d'un contrat d'achat ou pour la vérification d'éventuels droits à garantir. **Licite,** parce que le traitement des données s'effectue en vertu d'une relation contractuelle existante.
- L'entreprise envoie des publipostages par la poste à sa clientèle existante afin de faire de la publicité pour un produit nouvellement commercialisé. **Licite,** parce qu'il est permis d'utiliser des données de clients aussi à des fins de publicité.
- Utilisation de données à ses propres fins publicitaires bien que le client ait déclaré ne pas vouloir recevoir de publicité. **Licite,** parce que, en cas d'opposition à la publicité, il n'est pas permis d'utiliser les données à cette fin.
- Une entreprise divulgue les coordonnées de tout son personnel sur Internet. **Licite,** parce qu'il n'est pas permis de divulguer que les coordonnées des membres du personnel avant des contacts avec l'extérieur.
- Un médecin transmet les données de ses patients à un fabricant de médicaments pour que celui-ci puisse faire une publicité ciblée pour ses médicaments. **Licite,** parce qu'il n'est pas permis d'utiliser des données particulièrement sensibles à des fins publicitaires.
- Une entreprise fait détruire des médias de stockage par un prestataire de services. **Licite,** lorsque les dispositions ont été mises en œuvre en vue du traitement de l'ordre.
- Une entreprise publie des photos de collaborateurs de la distribution sur son site Internet. **Licite,** à la condition que le collaborateur ait auparavant donné son consentement à la publication.
- Une entreprise a l'intention d'attirer par téléphone l'attention de ses clients (coordonnées) sur ses nouveaux produits. **Licite,** lorsque le client a donné son consentement à être publié par téléphone.

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.



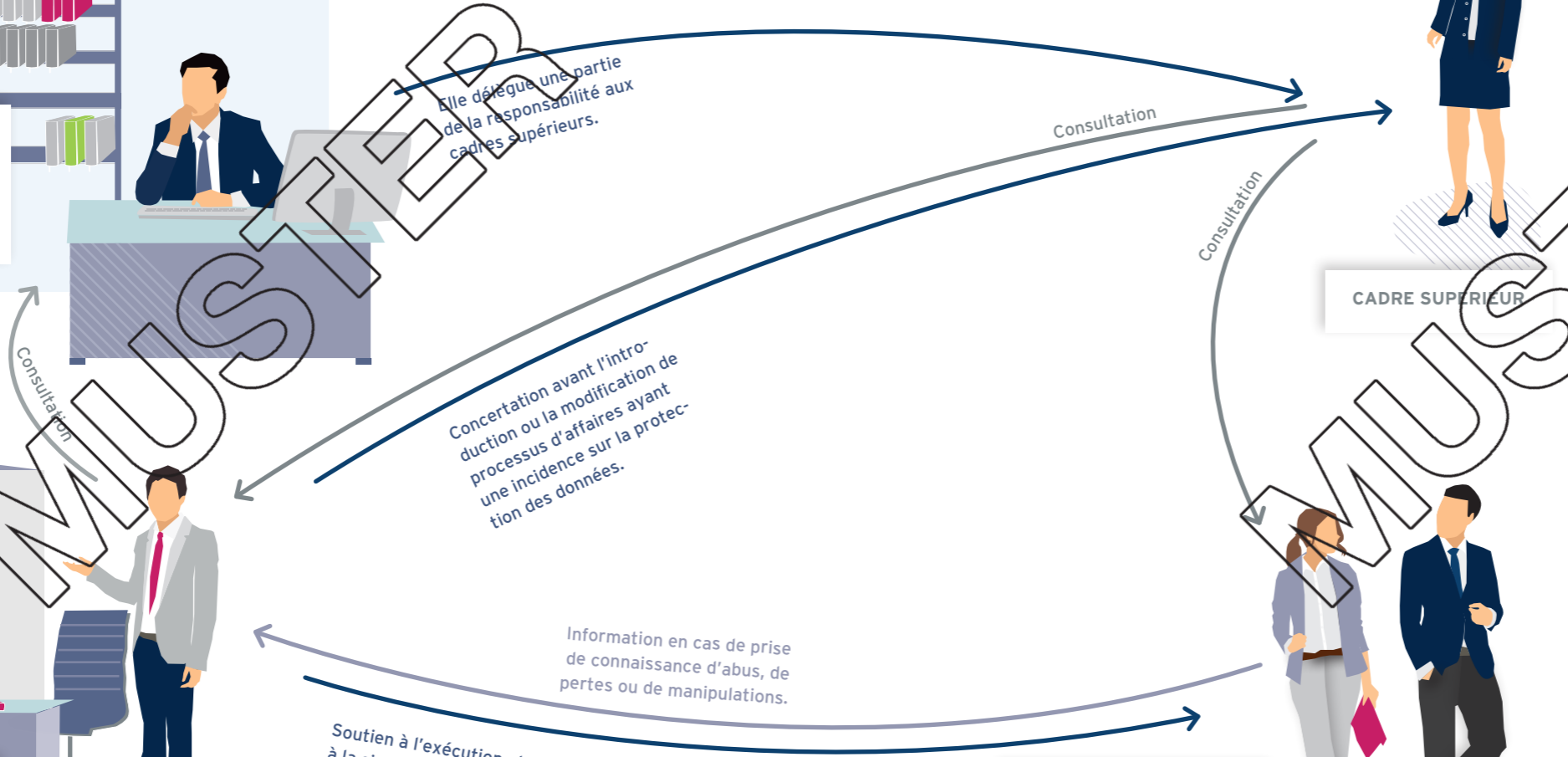
La protection des données comme mission des services spécialisés et des collaborateurs

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 à la sécurité des données par le biais de mesures techniques et organisationnelles appropriées.

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'entrée non autorisée dans les 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 ou 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 de 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

Constataction 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, plan de continuité 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.



Séclenner l'écran du système

Toujours séclenner 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^{ème} édition revue et actualisée 2018

© 2018 DATAKONTEXT GmbH, Frechen
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

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.

