ELO pour RGPD

Solutions et fonctionnalités pour la mise en œuvre
des dispositions du nouveau règlement général
européen sur la protection des données RGPD (2018)

Avec ELO, relevez avec succès le défi du RGPD de l'UE

Chers lecteurs,

Le 25 mai, le nouveau règlement général sur la protection des données (RGPD) de l'Union européenne est entré en vigueur et chaque entreprise, grande ou petite, est tenue de respecter ce règlement.

Certains attendaient depuis longtemps ce changement pour protéger les personnes à l'ère du numérique contre les fake news et l'utilisation abusive des données. Pour d'autres, il s'agit d'un « monstre à deux têtes » parfaitement exagéré qui pose, justement aux petites et moyennes entreprises, des défis énormes pour sa mise en œuvre.

Il ne fait aucun doute que la protection des données est importante et chacun sait que, dans ce domaine, des négligences ont souvent lieu. Ces dernières années, les nombreux scandales sur les données personnelles en sont la preuve la plus flagrante. Et pourtant, quasiment aucun autre nouveau règlement n'a suscité autant d'inquiétudes que le règlement général sur la protection des données de l'UE, qui est dorénavant appliqué.

Ce qui est, d'une part, certainement lié aux amendes théoriquement élevées allant jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial de l'entreprise concernée. Certains problèmes d' interprétation et le manque de pratique sont, d'autre part, à l'origine de ces inquiétudes. À l'exemple des articles 13 et 14, qui instaurent une obligation complète d'information avant la collecte de données personnelles. Des efforts qui sont en pratique difficiles à accomplir partout et qui devraient en décourager quelques-uns.

J'ai moi-même assisté à de nombreux ateliers et conférences sur le RGPD de l'UE proposés par des juristes en droit informatique et des spécialistes de la protection des données et à l'issue desquels les participants étant encore plus inquiets qu'avant. Souvent parce que des recommandations pratiques de mise en œuvre n'ont pas été données.

Je dois ici quand même saluer les autorités des Länder en charge de la protection des données, qui malgré un manque de personnel ont accompli un travail formidable en fournissant des explications compréhensibles ou des formulaires pratiques et des conseils précieux.

Nous souhaitons, par le biais de la présente brochure, non seulement vous apporter des informations pratiques et compactes sur les exigences principales du nouveau règlement général de l'UE sur la protection des données, mais aussi vous montrer de façon concrète l'assistance informatique et fonctionnelle que notre **ELO pour RGPD** peut vous apporter pour que vous soyez en mesure de relever avec succès le défi posé par les exigences du RGPD européen.

En espérant que notre brochure saura répondre à vos questions, je vous souhaite une bonne lecture !

Karl Heinz Mosbach
Directeur d'ELO Digital Office GmbH

Contenu

Aperçu du RGPD de l'UE 4

Quand le traitement des données personnelles est-il autorisé ? 6

Sauvegarde des droits des personnes concernées 8

Mesures pour la sécurité informatique 9

Aperçu des mesures organisationnelles les plus importantes 10

La bonne nouvelle : **ELO pour RGPD** 11

ELO pour RGPD – Aperçu des fonctions 13

ELO Business Solutions : RGPD européen déjà intégré dans notre système 14

> En dépit des efforts fournis dans l'élaboration du règlement européen général sur la protection des données, les clauses d'ouverture peuvent entraîner des différences à l'échelle nationale. En effet, les nombreuses clauses d'ouverture du règlement européen général sur la protection des données confèrent aux états membres une compétence législative, ce qui leur permet de prendre en compte les directives nationales. Les concepts peuvent donc différer d'un pays à un autre. Etant donné que cette brochure a été traduite à partir de l'allemand, elle ne prend pas en compte les différents règlements nationaux en matière de protection des données. Par conséquent, les informations que vous trouverez dans cette publication sont sans engagement, et non pas un conseil juridique. Même si ces informations ont été élaborées avec le plus grand soin, nous déclinons toute responsabilité quant à l'exactitude, l'exhaustivité ou l'actualité de celles-ci. Les remarques détaillées et les exigences mentionnées doivent être, si nécessaire, contrôlées par des conseillers juridiques afin de constater si elles sont appropriées aux exigences de votre entreprise.
>
> Merci de prendre en compte ces aspects lors de la lecture de la brochure et de noter que nous déclinons toute responsabilité.

Aperçu du RGPD de l'UE

RGPD de l'UE : la responsabilité des dirigeants est engagée

Même si la protection des données fait avant tout partie des missions des responsables informatiques et des délégués à la protection des données, c'est la direction des entreprises qui est responsable de l'application du RGPD de l'UE. Elle doit s'assurer que les mesures requises sont mises en œuvre dans leurs entreprises.

Par conséquent, la responsabilité (personnelle) est engagée, d'une part en raison des amendes potentielles élevées qui peuvent être prononcées par les autorités de surveillance. D'autre part parce que les employés en cas de manquements et de graves violations du RGPD européen peuvent engager une action en justice contre l'entreprise pour obtenir des dommages et intérêts en raison du préjudice moral subi.

Par conséquent :
La protection des données relève de la responsabilité des dirigeants ! Organiser les mesures requises est simple, les ignorer constitue une grave négligence.

Amendes et risques de mise en jeu de la responsabilité

Même si l'entrée en vigueur du RGPD de l'UE n'entraînera pas immédiatement une vague de procédures de sanctions avec à la clé des amendes élevées, les risques sont bel et bien existants, notamment en cas de graves violations. Ce que souligne le large barème d'amendes allant jusqu'à 4 % du chiffre d'affaires mondial de l'entreprise concernée ainsi que l'obligation de notification auprès de l'autorité de contrôle compétente dans un délai de 72 heures en cas de violation des données.

Dans le cas de Facebook et de l'immense scandale des données avec Cambridge Analytica, une amende potentielle allant jusqu'à 1,6 milliard de dollars aurait pu être prononcée. Cet exemple montre clairement la large marge de manœuvre des autorités de contrôle de protection des données, qui, rappelons-le, sont en droit d'effectuer des contrôles sans préavis. L'avenir nous dira comment cela fonctionnera en pratique. En cas de non-respect du RGPD, les entreprises encourent dans tous les cas le risque suivant : recevoir un avertissement de la concurrence ou être poursuivies en justice pour le préjudice moral subi par les personnes concernées ainsi que par d'anciens employés ou des clients contrariés.
Même si nous espérons que ces cas seront limités, il faut aussi s'attendre au contraire. Ces situations représentent, en effet, de nouvelles perspectives pour les cabinets d'avocats qui se sont spécialisés dans les avertissements.

Il est conseillé de mettre en œuvre les mesures requises pour le respect du RGPD de l'UE rien que pour échapper à de tels avocats.

Quand le traitement des données personnelles est-il autorisé ?

En principe, le traitement des données personnelles n'est pas autorisé, à moins de disposer d'une autorisation légale.
C'est le cas si…

1. … une personne donne explicitement et librement son consentement pour le traitement des données la concernant.

Il peut s'agir d'une signature sur un formulaire ou d'un simple clic dans le formulaire de consentement (opt-in) sur Internet. Il est alors important que la personne qui donne son consentement soit parfaitement informée sur la forme et la finalité de la collecte/du traitement des données (politique de confidentialité) et soit avertie qu'elle peut à tout moment retirer son consentement.

Lorsqu'une personne s'enregistre à une newsletter, il faut veiller à ce que l'adresse e-mail soit confirmée grâce au procédé double opt-in (confirmation supplémentaire de l'e-mail). Pour en apporter la preuve, le nom, la date, l'heure et l'adresse IP (ou le lieu) doivent faire l'objet d'un protocole dans le système. Cette procédure s'applique également aux cartes de visite lorsqu'elles sont saisies dans une base de données d'adresses/un fichier.

> **Remarque :**
> Il n'est pas nécessaire de demander leur consentement aux personnes concernées pour une base de données de coordonnées déjà existante si ces données ont été collectées avant le RGPD européen et conformément au droit en vigueur (95/46/CE) au moment de la collecte.

2. … les données doivent être enregistrées et traitées pour l'exécution d'une obligation contractuelle.

C'est bien entendu le cas dans le cadre de chaque relation client. Il est ici autorisé d'utiliser les données uniquement aux fins indiquées. En principe, tout transfert de données à des tiers sans consentement explicite est interdit. Si le transfert de données personnelles (par exemple à un transporteur) est requis pour l'exécution du contrat, les données peuvent évidemment être transmises. Il faut néanmoins le spécifier clairement dans la politique de confidentialité. Il convient de mentionner ici qu'un accord écrit sur le traitement des données doit être conclu avec les entreprises qui seront en charge de la sous-traitance pour le compte d'un responsable. En cas de sous-traitance (par exemple des services cloud, des prestataires externes, des fournisseurs de boutiques en ligne), la responsabilité des deux parties est engagée.

3. … la sauvegarde d'intérêts légitimes du responsable est requise.

Par conséquent, le traitement des données personnelles par des entreprises est autorisé (publipostage direct sur de nouveaux produits, avis clients, etc.), à moins que ne prévalent les intérêts de la personne concernée qui exigent une protection des données à caractère personnel. Le droit des personnes concernées doit bien entendu être également respecté. Il faut ici mentionner qu'il est autorisé de collecter et d'exploiter d'autres données aux fins poursuivies pour, par exemple, être en mesure de bien conseiller un client. La collecte et l'enregistrement de telles données ne requièrent donc aucun consentement supplémentaire.

4. Toujours important : l'obligation d'information !

Si des données personnelles sont collectées, les personnes concernées doivent au préalable être toujours informées en détail sur la politique de confidentialité correspondante en vigueur dans la société (articles 13 et 14). Ce qui est très facile à mettre en place sur les sites Internet peut rapidement poser problème au quotidien, par exemple lors de la prise d'un rendez-vous par téléphone chez un nouveau dentiste. Dans ce cas, l'ULD (centre régional indépendant pour la protection des données du Schleswig-Holstein) pense qu'il est suffisant de présenter clairement sur le site du cabinet médical la politique de confidentialité et de remettre au patient une fiche informative lorsqu'il se rend pour la première fois au cabinet. D'une manière générale, nous constatons que le contenu des articles 13 et 14 doit encore être clarifié.

5. Autres cas

Par souci d'exhaustivité, il importe de préciser que le traitement est considéré comme légal dans les cas suivants :

- exécution d'obligations légales
- protection d'intérêts vitaux des personnes concernées
- exécution d'une mission d'intérêt public.

- **Remarque sur le contrat régissant le traitement par un sous-traitant :**
  Si des données personnelles sont transférées à des tiers pour leur traitement, un contrat écrit régissant le traitement par le sous-traitant doit être conclu. En cas de prise de connaissance occasionnelle des données (prestation de transport, support technique/maintenance), aucun contrat régissant le traitement par le sous-traitant n'est requis. Bien qu'il s'agisse d'un contrat, ce dernier peut être conservé sous forme électronique (scan ou PDF).

En cas de données personnelles qui se réfèrent à une personne physique identifiée ou identifiable, le RGPD européen distingue deux catégories :

a) Donnés générales telles que des coordonnées (nom, adresse, téléphone, email, adresse IP, etc.)
b) Données personnelles sensibles portant sur des catégories particulières (telles que la religion, l'état de santé, des données biométriques, etc.). Le RGPD européen indique que ces données doivent faire l'objet d'une protection particulière.

Sauvegarde des droits des personnes concernées

Pour de nombreuses entreprises, la sauvegarde des intérêts des personnes concernées, qui ont été renforcés par le RGPD européen, constitue un véritable défi. Cette sauvegarde comprend essentiellement les points suivants :

1. Droit d'accès

En vertu du RGPD européen, chaque personne concernée a le droit d'obtenir dans un délai d'un mois des informations sur les données personnelles la concernant qui sont enregistrées. Bien souvent, les entreprises ne disposent d'aucune liste récapitulative ou d'outils pour pouvoir répondre rapidement à une telle demande. Des mesures techniques et organisationnelles sont donc nécessaires et des processus correspondants doivent être créés pour remédier à une telle situation. Avant de communiquer des données, il faut, dans tous les cas, s'assurer que la personne ayant formulé la demande est bien celle concernée par les données.

2. Droit à la portabilité

Chaque personne concernée a le droit d'exiger que ses données soient transmises et lui soient remises. Tant qu'il ne s'agit que de simples coordonnées, ce n'est sûrement pas un problème. Mais s'il s'agit de dossiers volumineux sur des clients, des patients et des chantiers ou bien encore d'échanges d'e-mails, la tâche sera plus ardue : sans assistance technique, compiler manuellement ces données prendra beaucoup de temps et, par conséquent, les coûts seront élevés. En cas de transfert de données, par exemple dans un dossier ZIP ou sur un support de données, il faut veiller à ce que ces données soient cryptées et que le mot de passe soit communiqué séparément (p. ex. par SMS ou par courrier postal).

3. Droit à l'effacement

En principe, chaque personne concernée a le droit d'exiger l'effacement de ses données dans la mesure où aucun délai de conservation légal ou aucune autre règle ne s'y oppose. À l'exemple des justificatifs commerciaux qu'il faut conserver pendant dix ans pour des raisons fiscales. Dans un tel cas, une autre loi prévaut sur le RGPD européen. Si l'effacement d'informations soumises à une obligation de conservation n'est techniquement pas possible (par exemple sauvegarde sur bande magnétique), l'accès à ces informations doit être limité ou bloqué.

Dans de nombreux cas, les prescriptions légales prévoient même explicitement l'effacement de données dans des délais précis si aucun consentement personnel n'a été donné. Les dossiers de candidature doivent, en général, être effacés au bout de trois mois. En revanche, des frais de déplacement remboursés dans un tel contexte ne pourront pas être effacés. Ils doivent être conservés pendant dix ans pour des raisons fiscales. Si nous jetons un œil sur les pratiques habituelles des entreprises, nous constatons que l'effacement ciblé des données n'a jusqu'à présent que peu progressé. Cette tâche était considérée comme trop chronophage et trop coûteuse. Par conséquent, de nombreuses entreprises conservent des données très anciennes qui n'ont plus aucune pertinence d'un point de vue légal ou du contenu. Ce qui n'est plus possible depuis l'entrée en vigueur du RGPD européen. Les entreprises doivent implémenter des solutions qui permettent l'effacement des données personnelles à l'expiration des délais de conservation (article 19) et également de consigner et de tracer cet effacement. Les personnes concernées disposent d'autres droits, notamment du droit de rectification, du droit d'accès et du droit d'opposition.

Autres droits des personnes concernées :

- **Droit à la rectification**
- **Droit à l'information**
- **Droit d'opposition**
- **Droit à la limitation**

Mesures pour la sécurité informatique

Garantir la sécurité informatique est un thème important pour les entreprises, et pas seulement depuis le nouveau RGPD de l'UE. Les conditions propices à la sécurité informatique sont déjà réunies depuis longtemps. Néanmoins, elles revêtent une autre importance en raison des amendes élevées qui peuvent être prononcées (par exemple en cas de violation de données). La mise en œuvre de mesures techniques et organisationnelles appropriées est ainsi obligatoire. Dans ce domaine, de graves lacunes sont encore identifiées dans des cas isolés, notamment dans les PME, par exemple des pare-feux non actualisés ou des sauvegardes sans historique qui peuvent être facilement écrasées. À cela s'ajoute des accès à des données en partie ouvertes ou des salles abritant les serveurs qui servent également d'espace de stockage de matériel et qui sont donc librement accessibles par tous les employés. Dans ce domaine, les exemples foisonnent. Avec l'introduction du RGPD européen, de telles négligences peuvent être lourdes de conséquences. Il est recommandé de contrôler méthodiquement la sécurité informatique et de consigner les mesures prises pour assurer cette sécurité informatique. Il est également conseillé de demander à un expert externe d'effectuer un audit. Il existe, dans ce domaine, suffisamment de listes de vérification et de guides. Ces mesures doivent, dans tous les cas, être considérées comme absolument nécessaires. En effet, le vol ou la perte de données peuvent entraîner des dommages financiers beaucoup plus importants.

Obligation de consignation

Quasiment chaque entreprise a l'obligation de tenir un registre des activités de traitement conformément au RGPD européen (article 30). Ce registre consigne les départements d'une entreprise et les systèmes (applications, bases de données, etc.) dans lesquels des données personnelles sont traitées. Les entreprises doivent également consigner les mesures techniques et organisationnelles qu'elles ont prises pour garantir le respect de leur politique de confidentialité.

La charge de travail, potentiellement importante, décourage de nombreuses entreprises, notamment celles de petite taille. Bien entendu, la tenue de ce registre requiert du temps. Mais, une approche collective et structurée permet de réduire le temps consacré à cette tâche. Notamment grâce aux remarquables modèles de formulaire (par exemple pour le registre des activités de traitement) que toutes les autorités de contrôle fournissent. Idem pour les mesures techniques et organisationnelles, pour lesquelles des listes de vérification et des formulaires sont disponibles. Si la charge de travail est répartie entre les départements et les personnes concernés, elle est alors limitée. Outre la mise en conformité avec les exigences du RGPD européen, la consignation présente un autre avantage pour les entreprises **:** la protection des données devient transparente et peut être tracée, qu'il s'agisse de données personnelles ou sensibles.

Évaluation d'impact de la protection des données

Si des données personnelles d'une catégorie particulière (données sensibles) et de nouvelles technologies sont utilisées à grande échelle (ces cas sont plutôt rares), une évaluation d'impact de la protection des données doit avoir lieu. Il s'agit essentiellement d'évaluer/d'analyser les risques relatifs à la sécurité informatique et aux processus.

Délégué à la protection des données

L'obligation de désigner un délégué à la protection des données fait l'objet de législations différentes dans les pays de l'UE. En Allemagne, les entreprises ont besoin d'un délégué à la protection des données si au moins dix personnes traitent des données personnelles en continu dans le cadre de leur activité principale (par exemple ventes, marketing, centre de traitement des commandes, etc.). Sont exclus les employés dont la mission principale ne consiste pas à traiter (saisir, enregistrer, etc.) des données personnelles, mais uniquement à avoir un contact occasionnel (par exemple des artisans, des mécaniciens, etc.). Si une entreprise doit désigner un délégué à la protection des données, soit un employé peut se qualifier en suivant une formation, soit un spécialiste externe peut prendre en charge cette mission. Ce qui est intéressant notamment pour les petites sociétés. Le délégué à la protection des données désigné doit être notifié à l'autorité de contrôle compétente (via son site Internet).

Aperçu des mesures organisationnelles les plus importantes

- ☑ Consigner les activités de traitement et les mesures techniques et organisationnelles
- ☑ Informer et former les employés
- ☑ Créer une charte (convention d'entreprise) sur le thème de la protection des données et de l'utilisation des données personnelles

  Recommandation : il convient ici de définir que les données privées ne doivent pas être mélangées aux données de l'entreprise. Il est, par exemple, conseillé d'interdire l'envoi d'e-mails privés avec la messagerie électronique de l'entreprise et il est recommandé de séparer et de supprimer immédiatement les e-mails privés reçus.
- ☑ Conserver la preuve du consentement (protocole : nom, date, adresse IP, lieu, etc.)
- ☑ Établir un contrat écrit avec les sous-traitants (tiers externes)
- ☑ Désigner, si nécessaire, un délégué à la protection des données et en informer l'autorité de contrôle compétente
- ☑ Contrôler et optimiser les autorisations d'accès, les cryptages et la sécurité générale
- ☑ Actualiser la politique de confidentialité, notamment les clauses concernant l'obligation d'information et les droits des personnes concernées

Relation avec les autorités de contrôle

En principe, les autorités de contrôle n'ont pas pour mission de prononcer des sanctions, elles conseillent de la même façon toutes les entreprises sur toutes les questions en relation avec le RGPD européen. Les autorités disposent, néanmoins, de larges pouvoirs, par exemple la possibilité d'effectuer des contrôles et des vérifications sans préavis. Il est extrêmement important que les entreprises signalent dans un délai de 72 heures toute violation de données (par exemple le vol de données) à l'autorité de contrôle. Une violation de données ne devrait jamais être dissimulée. Le cas échéant, l'entreprise concernée encourt très probablement une amende élevée.

La bonne nouvelle : ELO pour RGPD

Pour tous les utilisateurs des solutions ELO et ceux qui souhaitent encore le devenir, nous avons une bonne nouvelle : ELO est une plateforme parfaite pour mettre en œuvre et respecter les exigences du RGPD de l'UE. De nombreux détails fonctionnels tels que les délais d'effacement, des champs globaux de données personnelles, une base de données sur le traitement, des formulaires standardisés et beaucoup d'autres éléments ont été intégrés dans l'**ELO ECM Suite 11 : ELO pour RGPD**, notre solution pour la protection des données personnelles.

Fonction standard : identifiant de données personnelles

À l'heure actuelle, les données personnelles sont dispersées dans tous les départements d'une entreprise, que ce soit dans des comptes de messagerie électronique, des bases de données ou dans des dossiers quelconques contenant des fichiers. Si une personne souhaite avoir accès aux données personnelles enregistrées la concernant, l'entreprise se trouve confrontée à une tâche qui prend énormément de temps et aux coûts correspondants.

Afin d'éviter une telle situation, ELO a implémenté à partir de la version 11 de sa ECM Suite un identifiant appelé « Données personnelles » dans son modèle de données. Cet identifiant unique pour chaque personne (nom, le cas échéant numéro de personnel, numéro de client, etc.) peut dorénavant être ajouté à chaque document, chaque fichier et dans toutes les métadonnées, dans tous les processus et les services. D'un simple clic, il est possible de voir les données enregistrées relatives à une personne (client, client potentiel, etc.). Les données sensibles (données sur les employés) peuvent évidemment n'être consultées qu'avec les autorisations d'accès adéquates (cryptage).

Marqueurs de suppression et de conservation

La **ELO ECM Suite 11** comprend une nouveauté : le champ de marquage global « Fin du délai de suppression ». Avec le champ « Fin du délai de conservation », il gère un processus d'effacement automatique : les données anciennes ou obsolètes peuvent ainsi être automatiquement supprimées comme toute autre information qui devraient l'être en vertu du RGPD de l'UE. Accomplir une telle tâche manuellement nécessiterait un temps important et engendrerait des coûts élevés.

Avec ELO, l'exécution de ce processus est fiable et automatisée et fait, en outre, l'objet d'une journalisation de sorte que la transparence sera toujours assurée et que l'entreprise pourra répondre aux demandes d'accès des personnes concernées. Des délais de conservation légaux sont en même temps pris en compte : pour les justificatifs commerciaux qui doivent être conservés plus de dix ans, ce délai exclut toute demande de suppression tant que la durée de conservation minimale n'a pas été atteinte.

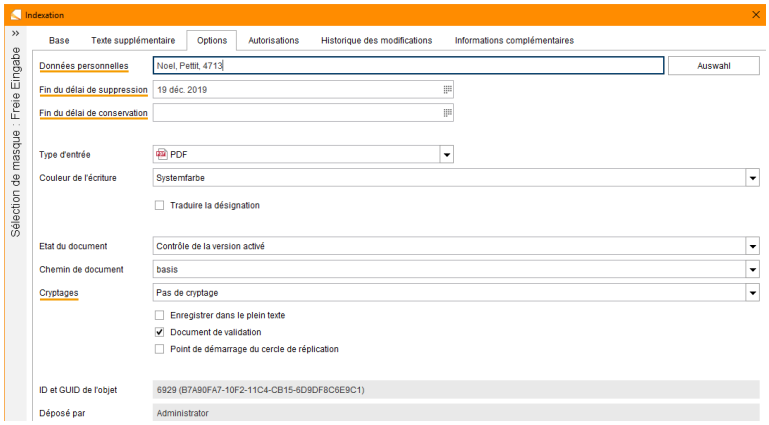


Illustration :

Champs de données RGPD dans l'**ELO ECM Suite 11**

Sécurité et finalité

Le nouveau règlement général de protection des données de l'UE prescrit la « protection sur la vie privée dès la conception » (privacy by design). ELO a placé la protection des données au cœur de son produit et fournit dans son système standard de nombreuses fonctions de protection des données notamment dans les Business Solutions spécialisées telles que le dossier RH électronique ainsi que la gestion du recrutement, des visiteurs et des contrats. De plus, il est possible de gérer pour tous les autres processus commerciaux et organisationnels la finalité et les restrictions d'accès à l'aide du système d'autorisation et de classification. Il est recommandé de crypter les données, notamment lorsqu'elles sont sensibles.Implémenter un tel cryptage est, pour de nombreux autres systèmes, complexe et requiert souvent des composants additionnels. Ce n'est pas le cas pour le système ELO, dont le périmètre standard inclut déjà une telle fonctionnalité. Il est par exemple possible de crypter les données sur les employées dès leur création, et d'en restreindre l'accès à un groupe déterminé de personnes. Dans l'hypothèse d'un vol de données, aucune information ne pourra être exploitée, dans la mesure où elles sont protégées par un chiffrement 128 bits.

Base de données de modèles de formulaires ELO pour une documentation simplifiée des processus

La charge de la preuve prescrite par le RGPD de l'UE implique une forte obligation de consignation pour les entreprises : qu'il s'agisse des mesures techniques et organisationnelles pour la sécurité des données et des processus, d'un contrat régissant le traitement par un sous-traitant en cas de transfert de données à des tiers ou de la consignation détaillée des départements d'une entreprise qui travaillent avec des données personnelles et de la manière de traiter ces données.

Pour faciliter le travail de ces entreprises, **ELO pour RGPD** propose un grand nombre de modèles de formulaires qui peuvent être très aisément adaptés aux besoins individuels. Il s'agit plus exactement d'une base de données de modèles de formulaires ELO, qui permet une création automatique avec des textes standard prédéfinis et une gestion des modifications simplifiée et traçable. Autre avantage de cette base de données : la possibilité d'analyser et d'évaluer simplement des champs dans un tableau de bord à l'aide des composants **ELO Analytics**. Il est, par exemple, possible de créer en un clic un aperçu qui présente les services dans lesquels des données sur des employés, des clients ou des patients d'une catégorie particulière sont traitées.

Création automatique de la cartographie du système

Dans le cadre des mesures techniques et organisationnelles, la création d'une cartographie du système constitue une tâche complexe pour de nombreuses entreprises. Qu'il s'agisse de la consignation des structures d'autorisation qui définit qui peut accéder à quelles données ou de la description de processus d'autorisation ou de processus précis, qui indique quand des données peuvent par exemple être effacées et bien d'autres situations. Ici aussi, **ELO pour RGPD** vous apporte son assistance en fournissant des documents de consignation et des analyses créés automatiquement.

Portabilité des données avec la fonction d'exportation ELO

Le nouveau règlement général sur la protection des données de l'UE prescrit que chaque personne concernée a, d'une part, le droit d'obtenir l'accès aux données personnelles enregistrées la concernant et, d'autre part, elle peut exiger que ces données soient transférées, par exemple en cas de changement de fournisseur de prestations.

Pour ce faire, ELO propose une fonction d'exportation automatisée des documents, des métadonnées, etc. Cette fonction permet, en un clic, d'exporter sous forme cryptée des données enregistrées sur une personne afin de permettre leur accès par email, par téléchargement ou au moyen d'un support de données. En outre, une lettre d'accompagnement (Transmittal Letter) peut être créée, indiquant en détail les données transmises et leur version.

ELO pour RGPD – Aperçu des fonctions

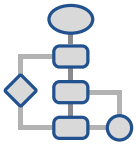
Protection par cryptage / autorisations

Identification spécifique des données personnelles

Traçabilité des processus concernés

Répartition des données par finalité

Suppression automatisée (cycle de vie)



Processus/ Approbation/ Autorisations

Export spécifique (portabilité des données)

Tableaux de bord (rapports/ justificatifs/ supervision)

Tableau de bord central pour la gestion des données relative au RGPD

Au vu du grand nombre d'exigences posées par le nouveau règlement général sur la protection des données de l'UE, il devient rapidement évident que l'on perd très vite pied sans une solution informatique. D'autant plus qu'il faut pouvoir immédiatement démontrer la transparence et la traçabilité de la gestion des données personnelles au cours de l'activité courante et en cas de contrôle. C'est là qu'intervient le tableau de bord RGPD proposé par ELO, qui permet pour tous les responsables de représenter visuellement et dans des graphiques clairement structurés tous les aspects de la gestion de la protection des données : étendue, nombre de données personnelles, processus de traitement et services de l'entreprise traitant ces données, audits réalisés, gestion des modifications et des patchs et bien d'autres informations. La direction et le délégué à la protection des données peuvent ainsi se servir de ce tableau de bord comme d'un outil de gestion centrale de la protection des données.

Gestion des e-mails ELO

Les boîtes e-mail et les sauvegardes correspondantes du système constituent, aujourd'hui, de véritables « cimetières de données », dans lesquels des données personnelles sont enregistrées bien au-delà des durées de conservation légales. Avec la gestion des e-mails ELO, vous pouvez remédier à ce problème : les e-mails peuvent être attribués à des processus commerciaux en fonction de l'activité et de la finalité, et ils sont automatiquement supprimés à l'expiration de leur délai de conservation et conformément aux prescriptions.

ELO Business Solutions : RGPD européen déjà intégré dans notre système

Les **ELO Business Solutions** sont des solutions standardisées qui permettent une réalisation de projet très rapide. Elles boostent non seulement votre activité, mais assurent également la sécurité de vos processus en conformité avec le RGPD européen.

Solutions RH numériques d'ELO : dossiers RH et gestion du recrutement

Dans chaque entreprise, les ressources humaines constituent un domaine dans lequel des données sensibles d'une catégorie spéciale sont traitées. De nombreuses entreprises, notamment les PME, auraient souvent besoin d'une solution de gestion professionnelle des ressources humaines. Les dossiers RH numériques **ELO HR Personnel File** et la solution de gestion du recrutement **ELO HR Recruiting** peuvent combler cette lacune et compléter les systèmes de ressources humaines déjà utilisés. Avec des logiques correspondantes propres à ce domaine et des processus standardisés, ces solutions vous aident à créer des processus de travail plus efficaces et plus fiables.

Gestion numérique de contrats : ELO Contract

Les contrats, notamment ceux conclus avec des particuliers, contiennent toujours des données à caractère personnel. En pratique, les documents contractuels sont souvent gérés dans des emplacements extrêmement divers (disques durs, dossiers de fichiers, supports de données mobiles) et sans aucune méthode harmonisée. Personne ne sait alors qui a enregistré une copie d'un contrat et où. **ELO Contract** permet non seulement aux départements spécialisés d'une entreprise de bénéficier d'une solution centrale de gestion de contrats, avec laquelle les contrats peuvent être gérés efficacement et en conformité avec la loi, mais leur fournit aussi une aide considérable pour le respect des exigences du RGPD de l'UE.

Gestion numérique des visiteurs : ELO Visitor

La gestion numérique et professionnelle des visiteurs proposée par ELO permet non seulement d'assurer un parfait suivi des visiteurs, mais aussi de répondre aux exigences principales du RGPD européen. Prenons, par exemple, le thème de la sécurité : **ELO Visitor** permet de créer rapidement des badges visiteurs, de contrôler les zones auxquelles les visiteurs ont accédé, quand et combien de temps ou bien encore de rédiger des instructions relatives à la sécurité, etc. Une visite suppose aussi que des données personnelles soient collectées (nom, société, numéro d'immatriculation, etc.), qui devront être supprimées à l'expiration d'un délai de conservation maximum. Là aussi, vous n'avez aucun souci à vous faire : **ELO Visitor** s'en charge pour vous.

Vous avez des questions sur la gamme de produits ELO et sur nos solutions assurant la conformité avec le RGPD?

› N'hésitez pas à nous contacter :
Téléphone : + 33 (0)1 85 76 11 44
E-mail : info@elo-digital.fr

ELO pour RGPD

Solutions et fonctionnalités pour la mise en œuvre des exigences du nouveau règlement général européen sur la protection des données RGPD (2018)

ELO® est disponible auprès de :

ELO Digital Office FR S.a.r.l., 102 Avenue des Champs-Élysées, 75008 Paris, France; info@elo-digital.fr
ELO Digital Office CH AG, Industriestr. 50b, 8304 Wallisellen, Suisse; info@elo.swiss
ELO Digital Office Benelux, Oktrooiplein 1, bus 201, 9000 Ghent, Belgium; elo-benelux@elo.com
ELO Digital Office GmbH, Tübinger Strasse 43, 70178 Stuttgart, Allemagne; info@elo.com

ELO Digital Office, le logo ELO, elo.com, ELOoffice, ELOprofessional et ELOenterprise sont des marques de ELO Digital Office GmbH en Allemagne et/ou dans d'autres pays.Microsoft ®, MS ®, Windows ®, Word ® et Excel ®, PowerPoint ®, SharePoint ®, Navision ® sont des marques déposées de Microsoft Corporation aux États-Unis et dans d'autres pays. Tous les autres noms de produits ou de services sont des marques déposées d'autres fournisseurs. Cette publication est uniquement destinée à fournir une information générale et ne peut en aucun cas remplacer un service de conseil individualisé. Les informations contenues dans cette publication peuvent être modifiées à tout moment sans annonce préalable. Les caractéristiques et fonctions techniques peuvent varier selon les pays. Vous pouvez obtenir des informations actuelles concernant les produits ELO, les conditions du contrat ainsi qu'une liste de prix auprès des sociétés ELO, auprès des partenaires Business ELO et/ou auprès des partenaires Channel ELO. Les informations sur les produits correspondent au développement actuel du logiciel. L'objet et l'étendue des prestations sont définis exclusivement conformément aux contrats correspondants. ELO ne garantit pas que ses produits ou autres prestations permettent de maintenir le respect de directives légales spécifiques en vigueur. Le client est lui-même responsable du respect des consignes de sécurité et des directives légales nationales et internationales. Les informations sont fournies sous réserve de modifications, d'erreurs et d'erreurs d'impression. Toute copie, reproduction ou transmission, intégrale ou partielle, sont autorisées uniquement avec l'autorisation écrite de ELO Digital Office GmbH © Copyright ELO Digital Office GmbH 2018. Tous droits réservés.
I 20180910

ELO® Digital Office