Livre blanc sur la sécurité de l’information

Conformité au RGPD

Introduction à la sécurité des données

www.sharp.fr

SHARP
Be Original.

Sommaire

Introduction

Pour toutes les entreprises, assurer la conformité au Règlement Général sur la Protection des Données (RGPD) de l'UE, particulièrement en ce qui concerne la protection des données personnelles, présente un certain nombre de défis.

Le Règlement Général sur la Protection des Données (RGPD) confronte les entreprises européennes à plusieurs défis.

Bien que le RGPD se focalise en grande partie sur la protection des données en ligne, il s'applique également à la façon dont les entreprises utilisent et stockent les données, ce qui signifie qu'elles doivent réfléchir à ce qu'il advient des informations qu'elles collectent (par le biais de la numérisation ou de la saisie électronique), qu'elles stockent et conservent, qu'elles traitent, qu'elles partagent, qu'elles impriment, qu'elles copient, qu'elles transmettent par fax et qu'elles archivent.

Ce règlement introduit des éléments précis telles que les Données personnelles, la Protection des données, l'Effacement des données, les Sous-traitants de données, les Responsables du traitement des données, les Délégués à la protection des données, la Conformité, l'Autorité chargée de la protection des données et bien d'autres encore (voir le Glossaire du RGPD, page 9).

Il existe de nombreuses publications qui expliquent comment interpréter les termes du RGPD, qui sera concerné et comment appliquer cette règlementation dans les entreprises. Toutefois, il n'existe qu'un nombre réduit de documents, d'articles ou de livres blancs qui expliquent comment traduire le RGPD en des termes vraiment parlants pour l'entreprise, et qui traitent de tous les processus liés aux activités de l'entreprise, particulièrement ceux liés aux données personnelles.

En associant les utilisateurs professionnels (employés), les processus métiers (flux de travail et bonnes pratiques) et les actifs d'entreprise (matériels et logiciels), Sharp a défini trois domaines distincts de la sécurité d'entreprise qui, lorsqu'ils sont réunis, peuvent améliorer la sécurité globale de l'entreprise et permettre de s'inscrire dans une démarche de mise en conformité au RGPD.
Ces trois domaines sont les suivants :

- **Sécurité des réseaux**
  Sécurité de tout réseau utilisé par une entreprise, géré par un service informatique, où l'accent est mis sur tous les matériels connectés permettant d'imprimer, de numériser et de transmettre des fax.

- **Sécurité des documents sortants**
  Sécurité des documents sortants, imprimés ou numérisés provenant de MFP ou d'imprimantes. Cette catégorie inclut tous les documents imprimés sur papier et les images de documents en transit entre un ordinateur et un matériel d'impression (y compris via des serveurs d'impression dédiés), la numérisation (y compris la numérisation vers un dossier, vers un e-mail, vers le Cloud) et le fax.

- **Sécurité des documents**
  Sécurité des informations capturées à partir de documents papier par le biais d'un processus de numérisation ou d'images électroniques des documents stockés dans les répertoires d'entreprise, par exemple les e-mails, fichiers électroniques, formulaires, etc.

Sharp peut accompagner les entreprises dans leur démarche de mise en conformité au RGPD en mettant en place et en appliquant un ensemble d'outils et de bonnes pratiques pour les processus métiers, directement liés à la sécurité des réseaux, des documents sortants et des documents en général.

Contexte

Le RGPD est le changement le plus important qu'ait connu le domaine de la protection des données depuis plus de deux décennies. Toutefois, nombre de questions demeurent, et les réponses sont limitées.

Le RGPD introduit de nouvelles exigences et définit les sanctions financières appliquées si les protections et les mesures préventives contre les violations sont insuffisantes[1]. En revanche, très peu de recommandations sont prodiguées sur ce que les propriétaires d'entreprises, les responsables informatiques et les utilisateurs doivent faire pour être en conformité. Il appartient à chaque entreprise de déduire ce qu'il faut mettre en place.

Le principal objectif de la mise en application du RGPD était de mieux gérer et de mieux protéger le traitement des données personnelles. Cela signifie que toutes les informations personnelles présentes sur vos systèmes d'entreprise – des coordonnées des clients ou des professionnels stockées sur les applications métier, à tous les paramètres réseau, comptes de gestion de documents et de gestion d'impressions, en passant par les documents RH sur le personnel – devraient être gérées de façon appropriée.

Il existe deux niveaux principaux de conformité au RGPD :

- **Niveau personnelle**
  Tous les aspects liés à l'utilisateur, y compris son comportement, sa manière de travailler et la façon dont les règles et systèmes d'entreprise sont appliqués à ce dernier.

- **Niveau organisationnelle**
  Les processus métier au sein d'une organisation (y compris les flux de travail papier et électroniques), les actifs (y compris ceux qui aident les employés à partager et à communiquer sur papier ou de façon électronique), la culture et comment elle réagit aux défis que présente le marché.

En mettant en place des stratégies et des outils au niveau de l'organisation, il est possible de définir et de gérer le changement attendu de comportement des utilisateurs finaux et la façon dont ils travaillent et traitent l'ensemble des données d'entreprise disponibles. Ceci permet de mieux comprendre comment traiter les documents et les données personnelles.[2]

Par conséquent, Sharp se focalise sur le niveau organisationnelle (processus, solutions et matériels) et peut contribuer à l'élaboration de politiques de sécurité complètes qui sont vitales pour chaque entreprise.

En se concentrant sur les trois domaines de la sécurité d'entreprise, Sharp a mis en évidence les risques potentiels qui pourraient entraîner des violations de la conformité s'ils ne sont pas traités :

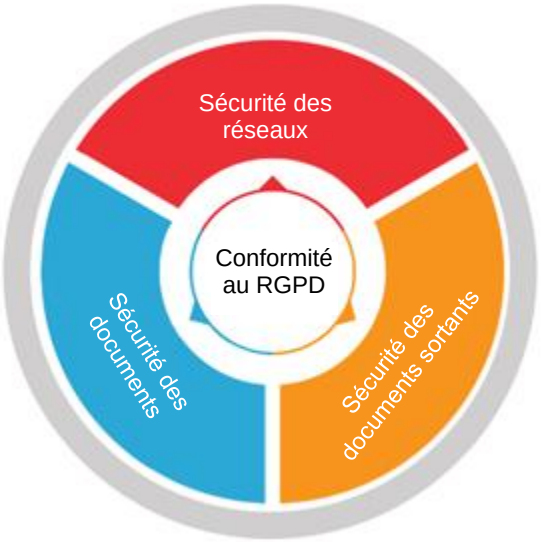
- **Risques liés aux réseaux**
  - Les vulnérabilités que présente le transfert de données du format papier au format électronique, puis de nouveau au format papier.
  - La nécessité de sécuriser les MFP et les imprimantes au même niveau que les serveurs, et la nécessité de mettre en place une politique d'impression sécurisée planifiée et unifiée.
  - La nécessité de surveiller et de gérer les périphériques afin de soutenir et de mettre à jour régulièrement, lorsque cela est nécessaire, la politique de sécurité en fonction des nouvelles vulnérabilités.
  - La nécessité d'éliminer les données de façon sécurisée et en temps voulu.

- **Risques liés aux documents sortants**

- La nécessité de sécuriser l'accès aux systèmes d'impression, afin de contrôler les documents sortants et l'acheminement des données confidentielles.
- Gérer le nombre et les types de documents sortants – copies, impressions, fax, numérisations (y compris la numérisation vers un e-mail et vers un dossier).
- La nécessité de disposer d'un journal d'audit pour pouvoir apporter la preuve de ce qui a été enregistré ou imprimé.

- **Risques liés aux documents**
  - Absence de définition et de compréhension du cycle de vie des documents dans l'entreprise. Ceci inclut toutes les étapes du cycle de vie du document, de la création du document à son élimination.
  - Les répertoires de documents non structurés et sécurisés qui laissent les systèmes de gestion documentaire vulnérables aux attaques et aux violations potentielles.
  - Tâches manuelles répétitives liées aux documents (électroniques et papier), où une mauvaise destination pourrait être ajoutée par erreur et entraîner des violations de données.
  - Partage non contrôlé de documents d'entreprise critiques.
  - Risque de corruption des données sans contrôle des versions.

Les 3 piliers de la conformité au RGPD selon Sharp



Recommandations

Grâce à son expertise en matière de sécurité, Sharp peut accompagner les entreprises dans leur démarche de mise en conformité aux règlementations les plus strictes, et crée des solutions permettant de gagner en efficacité.

Sharp a pour objectif d'accompagner les entreprises dans chaque aspect de la sécurité de l'information en couvrant trois domaines principaux : la sécurité des réseaux, la sécurité des documents sortants, et la sécurité des documents en général. Nous couvrons les aspects organisationnels du traitement des données et de leur protection au travers de notre offre complète de produits et de solutions optimisés, et de nos Services professionnels Sharp associés.

En développant une base solide dans l'ensemble de la couche organisationnelle d'une entreprise, nous pouvons influencer le comportement de l'utilisateur final. Conjointement avec nos systèmes sécurisés et bien conçus, ceci aide les entreprises à se conformer au RGPD et fournit les outils appropriés pour mesurer le risque, empêcher les cyberattaques et récolter des informations précises sur les utilisateurs.

Les compétences de Sharp couvrent tous les aspects de la sécurité des données, y compris la façon dont les données personnelles sont utilisées dans les systèmes métier, ce qui aide les organisations à se conformer au RGPD.

Voici un tableau récapitulatif qui montre comment Sharp peut vous accompagner dans votre démarche de mise en conformité au RGPD :

Règlement Général sur la Protection des Données et Sharp		
Aspect/domaine de la sécurité	Produits et solutions	Conformité par le biais de
Sécurité des réseaux	• MFP Sharp • Imprimantes Sharp • Sharp Remote Device Manager	• Contrôle de l'accès utilisateur • Contrôle des ports • Contrôle des protocoles • Contrôle des services réseau • Chiffrement des données • Écrasement des données
Sécurité des documents sortants	• Job Accounting II • PaperCut MF • SafeQ • Drivve Image	• Contrôle de l'accès • Restrictions des fonctionnalités accessibles • Journal des données / Rapport d'audit • Conservation et effacement du journal des données
Sécurité des documents	• Cloud Portal Office • Drivve DM • Docuware • Drivve Image	• Contrôle de l'accès aux bases de données • Contrôle des droits des utilisateurs

		• Suivi des versions • Journal d’audit • Conservation des documents, et élimination des documents

Conclusion

Sharp peut aider les organisations à mettre en place des mesures de sécurité et des méthodes de gestion efficaces qui contribuent à une mise en conformité au RGPD.

Comprendre, planifier, et exécuter les mesures permettant la conformité au RGPD peut prendre beaucoup de temps et entraîner de réelles difficultés de mise en œuvre, notamment parce que chaque entreprise a ses spécificités.

Sharp recommande aux propriétaires d'entreprises et aux responsables informatique de consulter les livres blancs proposés dans notre bibliothèque pour obtenir des conseils au sujet des trois thématiques que sont la sécurité des réseaux, la sécurité des documents sortants et la sécurité des documents

Ces livres blancs décrivent les risques et les mesures préventives, et présentent :

- Les matériels réseau sécurisés de Sharp ;
- Les solutions logicielles de Sharp qui contribuent à protéger la capture et la sortie des données d'entreprise ;
- Les solutions logicielles de Sharp qui contribuent à la protection des documents électroniques.

En outre, l'équipe Sharp Professional Services offre des prestations de conseil et aide à définir des mesures de sécurité solides et à mettre en place des outils pertinents pour chaque type d'entreprise et chaque besoin.

Pour éviter les vulnérabilités potentielles dans d'autres domaines de votre organisation, nous pouvons vous aider à mettre en œuvre des mesures de sécurité supplémentaires issues de l'offre Sharp, afin que vous puissiez assurer une sécurité à 360 degrés pour chacun des domaines identifiés au sein de votre :

- Sécurité des réseaux ;
- Sécurité des documents sortants;
- Sécurité des documents ;
- Conformité au RGPD.

Glossaire du RGPD[3]

Responsabilité – Le responsable du traitement des données est responsable de la conformité aux principes de protection des données. Il doit être en mesure de démontrer les mesures prises par l'entreprise pour garantir la conformité aux différents règlements.

Violation des données – Toute destruction, perte, altération, divulgation non autorisée ou accès accidentel ou illégal à des données d'une personne.

Responsable du traitement des données – « Responsable » signifie la personne morale, l'autorité publique, l'agence ou autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données personnelles.

Effacement des données (également appelé « Droit à l'oubli ») – Ceci donne le droit à la personne concernée de demander à ce que le responsable du traitement des données efface ses données personnelles.

Sous-traitant de données – La mission du sous-traitant de données porte sur le traitement des données, à savoir toute opération réalisée sur les données personnelles ou sur des ensembles de données personnelles. On parle de traitement que ces opérations soient réalisées manuellement ou de façon automatisée. Le traitement comprend les activités suivantes : collecte, enregistrement, organisation, utilisation, structuration, stockage, adaptation, récupération, consultation, destruction et plus encore. Le sous-traitant de données peut être une organisation ou un fournisseur tiers qui gère et traite les données personnelles au nom du responsable du traitement des données. Les sous-traitants de données sont tenus par certaines obligations légales spécifiques, telles que la tenue à jour de dossiers personnels, et sont responsables en cas de violation de données.

Autorité chargée de la protection des données – L'autorité nationale qui protège la confidentialité des données.

Délégué à la protection des données – Personne désignée dont le travail consiste à s'assurer que vous mettez en œuvre les politiques et procédures établies par le RGPD, et vous y conformez.

Personne concernée – Personne dont les données personnelles sont traitées par un responsable du traitement des données ou un sous-traitant de données.

Données personnelles – Toute information directe ou indirecte relative à une personne identifiée qui pourrait être utilisée comme moyen permettant de l'identifier. Ceci comprend son nom, son numéro de document d'identité, ses données de localisation ou un identifiant en ligne.

Traitement – Ce terme se rapporte à toute activité relative aux données personnelles, de leur collecte initiale à leur destruction finale. Ceci comprend l'organisation, l'altération, la consultation, l'utilisation, la divulgation, l'association et la rétention des données, que ce soit manuellement ou de façon électronique.

Références

1. « UK firms could face £122bn in data breach fines in 2018 » (Les entreprises britanniques pourraient payer 122 milliards de livres d'amendes pour violation de données en 2018), ComputerWeekly, octobre 2016
2. « CEO Survey » (Enquête auprès des PDG), PwC, 2017
3. « GDPR Glossary of Key Terms » (Glossaire des termes clés du RGPD), High Speed Training, février 2018

SHARP

Be Original.