



RGPD

Règlement Général sur la Protection
des Données

Passer la ligne d'arrivée de la RGPD



Sommaire

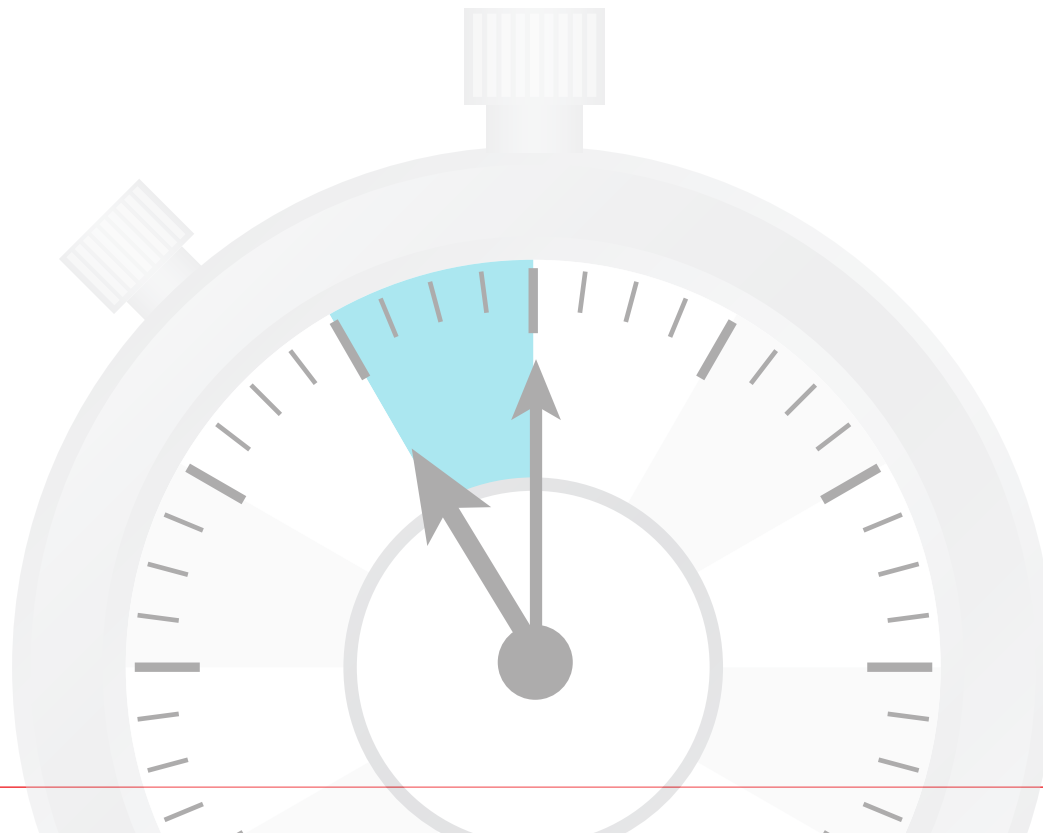
C'est une course contre la montre !	3
Qui est concerné ?	4
Que considère-t-on comme des données à caractère personnel ?	5
Attention aux obstacles sur la route	6
Notifications de violation de données	6
Consentement explicite	6
Transfert des données en dehors de l'UE	6
Désignation d'un Délégué à la protection des données	7
Sanctions/coûts liés à la non-conformité	7
La stratégie gagnante	8
Franchissez la ligne d'arrivée	9
Checklist de la planification RGPD	14

C'est une course contre la montre !

Avec l'adoption en avril 2016 du règlement (EU) 2016/679, communément appelé Règlement Général sur la Protection des Données (RGPD), des entreprises comme la vôtre participent aujourd'hui à une course à la conformité avant son entrée en vigueur le **25 mai 2018**, sous peine d'amendes, voire de poursuites judiciaires. Cette course est particulièrement longue et difficile car le Règlement étend considérablement le cadre de responsabilité défini par la Directive de 1995 sur la protection des données (Directive 95/46/EC) précédemment appliquée.

La bonne nouvelle c'est que **vous n'êtes pas seuls !** Tout comme le peloton d'une course cycliste, la plupart des entreprises sont au même point dans le processus de conformité et nous franchirons la ligne d'arrivée plus vite et plus facilement en faisant équipe.

Le Règlement
Général sur la
Protection
des Données
entre en vigueur le
25 mai 2018



Qui est concerné ?

Ce livre électronique a pour but de partager des informations clés sur le règlement RGPD et d'offrir des solutions pour accompagner vos projets de mise en conformité et améliorer la sécurité de vos données.

Les entreprises qui collectent, conservent et/ou traitent des informations personnelles doivent appliquer le règlement RGPD si elles :

- offrent des produits ou services à des citoyens de l'UE résidant dans l'UE

OU

- surveillent le comportement de citoyens de l'UE résidant dans l'UE

Ainsi, les entreprises qui ne sont ni basées ni présentes dans l'UE sont concernées, tout comme celles employant des citoyens de l'UE, mais sans clients dans l'UE.

Dans la mesure où vous traitez des informations personnelles concernant des citoyens de l'UE, vous êtes concernés !

Toutes les entreprises qui répondent à ces critères doivent se conformer au règlement. Toutefois, celles qui traitent un grand nombre de données doivent satisfaire un plus grand nombre d'exigences.

Dans le Règlement, les entreprises soumises à son application sont appelées « responsables du traitement » ou « sous-traitants ». Les responsables du traitement sont les entités qui déterminent l'objet, les conditions et les modes de traitement des données personnelles, alors que les sous-traitants sont celles qui traitent les données personnelles pour le compte du responsable du traitement.

Par exemple, une clinique externalise ses analyses de laboratoire à un autre établissement. Elle doit partager un certain nombre des informations personnelles qu'elle a collectées avec le laboratoire pour pouvoir renvoyer les résultats au patient approprié. Dans ce cas, la clinique est le responsable du traitement et le laboratoire est le sous-traitant selon les critères de la RGPD. Les critères de la RGPD diffèrent pour chaque rôle, vous devez donc déterminer si votre entreprise est concernée par un seul des rôles ou les deux.

Que considère-t-on comme des données à caractère personnel ?

Le règlement RGPD donne une définition large des données à caractère personnel. Toute donnée susceptible d'être utilisée pour identifier directement ou indirectement une personne est considérée comme une « donnée à caractère personnel ». Cela englobe aussi bien les noms, les photos, les adresses e-mail, les coordonnées bancaires, les numéros de sécurité sociale, les messages sur les réseaux sociaux et les données médicales que les adresses IP des ordinateurs associés aux comptes ou aux appareils des utilisateurs.

Par exemple, si vous organisez une course et capturez ou affectez des numéros de dossard dans un système informatique, et que ces numéros sont associés à une personne, il s'agit de données à caractère personnel. De plus, ces numéros sont souvent facilement recoupés avec des données personnelles, telles que le nom, l'adresse, la photo, la condition physique d'avant-course et autres informations sur le participant.



Le peloton Photo :
Sue Hixson



Attention aux obstacles sur la route

Le règlement RGPD inclut un certain nombre d'éléments non présents dans la précédente directive sur la protection des données, qui peuvent vous surprendre si vous n'y prêtez pas attention. Voici une description de certaines des nouveautés les plus significatives, mais reportez-vous au Règlement pour plus de détails et la liste complète.

- **NOTIFICATIONS DE VIOLATION DE DONNÉES** : Les responsables du traitement et les sous-traitants doivent désormais informer les autorités de contrôle dans les 72 heures suivant la découverte d'une violation, ainsi que les personnes à qui appartiennent les données (personnes concernées) « sans retard excessif ».

Notez qu'une violation de **données chiffrées** est **expressément exclue** des exigences de notification. Vous devez donc en tenir compte dans votre stratégie de conformité.

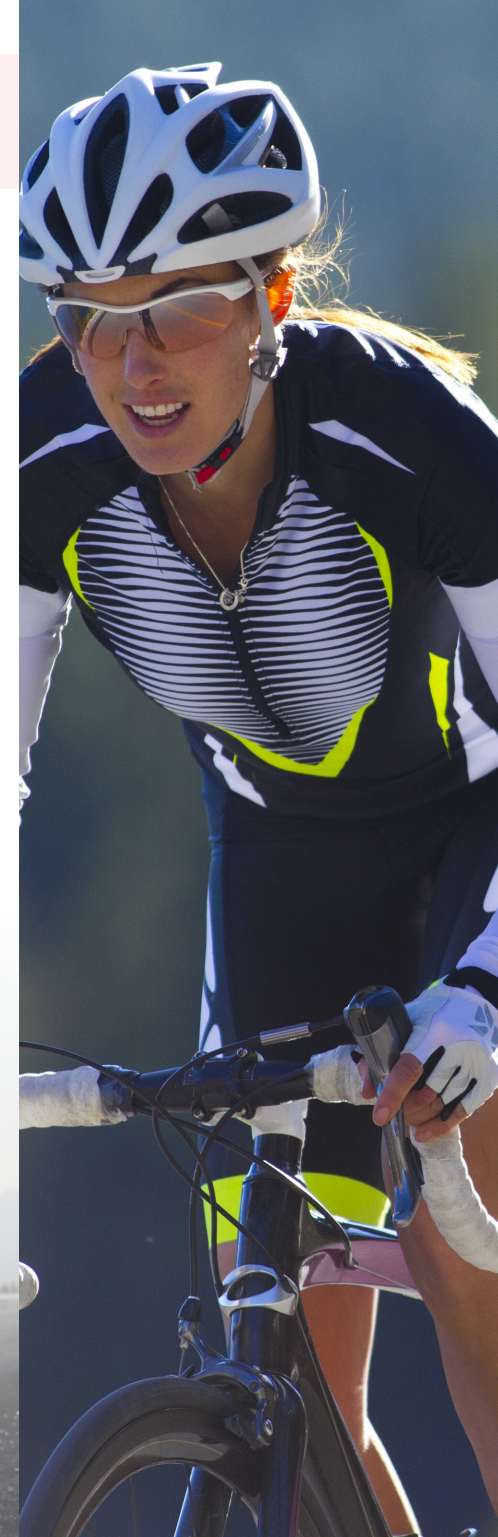
- **CONSENTEMENT EXPLICITE** : Le règlement RGPD exige qu'au moment de collecter les données personnelles, un consentement explicite soit donné par la personne concernée. Ainsi, les entreprises ne peuvent plus intégrer de consentement générique dans un jargon juridique incompréhensible. À la place, elles doivent fournir des informations spécifiques sur les données collectées, leur stockage et leur traitement, et ce, dans un langage clair et simple. Dans ce contexte, un simple « j'accepte » répond tout à fait aux critères du règlement. De plus, il doit être tout aussi facile de retirer son consentement que de le donner.
- **TRANSFERT DES DONNÉES EN DEHORS DE L'UE** : Les données à caractère personnel ne peuvent pas quitter l'UE sauf accord de l'autorité de contrôle, ou lorsque la personne concernée est informée de ce transfert et des risques associés, et l'autorise.



- **DÉSIGNATION D'UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES** : Si vous traitez un grand nombre de données, vous devez désigner (embauche, affectation ou services externes) un délégué à la protection des données pour votre entreprise. Le Délégué est votre représentant auprès des autorités de contrôle qui supervisent et garantissent l'application du Règlement. Il ou elle doit aussi répondre à toutes les demandes ou réclamations émises par les personnes concernées. De plus, le Délégué dirige vos activités de conformité, telles que requises suite à l'analyse d'impact relative à la protection des données et gère la communication liée aux stratégies de sécurité, aux évaluations, à la conformité, aux demandes des personnes concernées et aux notifications de violations, entre autres. Conformément au règlement, le délégué agit sous l'autorité du directeur exécutif et est désigné pour une période reconductible de deux ans.

- **SANCTIONS/COÛTS LIÉS À LA NON-CONFORMITÉ** : Les entreprises qui ne respectent pas le règlement RGPD encourent une amende pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondial. Les amendes sont appliquées et évaluées dès la première infraction et peuvent représenter 2 % du chiffres d'affaires mondial pour tenue de registres inappropriée (Article 28), par exemple. Par ailleurs, les entreprises encourent des frais supplémentaires, y compris des honoraires juridiques et réparations judiciaires, si les citoyens de l'UE estiment que leurs droits ont été violés, intentent un procès pour dommages et le remportent.

Les entreprises
encourent une
amende pouvant
aller jusqu'à
20 millions €
ou **4 %** du chiffre
d'affaires mondial



La stratégie gagnante

La mise en conformité RGPD exige un effort considérable de la part de pratiquement toutes les entreprises et inclura certainement :

- Des mesures de protection des données **basées sur la technologie de sécurité du réseau la plus** performante qui :
 - **protège les données** pendant leur stockage et leur transmission
 - garantit **la sensibilisation situationnelle** aux risques
 - permet **une action préventive, corrective et d'atténuation en quasi temps réel** en cas de détection de vulnérabilités ou d'incidents susceptibles de présenter un risque pour les données
 - inclut **des outils d'évaluation de l'efficacité** des stratégies de sécurité.
- Un système de récupération des données qui restaure l'accès aux données en cas d'incident affectant la disponibilité
- Des processus et structures de génération de rapports nouveaux ou améliorés pour effectuer le suivi du consentement, des notifications de violation et de la conformité

Vous devez aussi identifier les possibilités de réduction du cadre/risque de l'impact RGPD afin de réduire les activités liées à la surveillance, à la tenue de registres et à la conformité exigées par le règlement RGPD.

Par exemple :

- **Réduire** le nombre de champs de données personnelles collectés/traités
- **Réduire** la durée de conservation/traitement des données personnelles
- **Chiffrez les données** inactives et en transit
- **Masquez les adresses IP** et anonymisez les autres types de données utilisateur
- **Réduire** le nombre de personnes autorisées à accéder à ces données personnelles
- **Augmentez** les moyens de prévention et d'élimination des menaces sur les données personnelles

Nous avons inclus une checklist de planification RGPD à la fin de ce livre électronique pour vous aider à démarrer.

La checklist et les questions qui l'accompagnent vous permettent d'évaluer les politiques et pratiques de sécurité actuelles pour identifier les critères du règlement RGPD respectés et non respectés.

Franchissez la ligne d'arrivée !

Maintenant que vous savez comment commencer votre projet de mise en conformité RGPD, vous allez sans doute chercher à résoudre les difficultés avec des solutions rapides et simples de mise en conformité RGPD pour pouvoir terminer cette course dans les délais. WatchGuard peut vous aider à atteindre la conformité grâce à une technologie et des pratiques de sécurité très efficaces.

De plus, nous vous avons facilité la tâche. WatchGuard fournit les mesures de sécurité des données nécessaires à la mise en conformité RGPD, et ce, dans une solution unique et simple d'utilisation avec la suite Total Security. Offrant une sécurité d'entreprise renforcée, les appliances de sécurité WatchGuard Firebox® dotées de la suite Total Security incluent 16 des 20 principaux contrôles de sécurité SANS (v6) pour offrir un produit complet nécessaire à la conformité RGPD.

Une appliance de sécurité WatchGuard Firebox avec la suite Total Security
inclut **16 des 20 principaux** contrôles SANS

20 principaux contrôles de sécurité SANS V6

CS1	Inventaire des appareils autorisés et non autorisés	Oui	CS11	Configurations sécurisées pour les périphériques réseau, tels que pare-feux, routeurs et commutateurs	Oui
CS2	Inventaire des logiciels autorisés et non autorisés	Oui	CS12	Défense du périmètre	Oui
CS3	Configuration sécurisée pour les matériels et logiciels sur appareils mobiles, ordinateurs portables, postes de travail et serveurs	Oui	CS13	Protection des données	Oui
CS4	Évaluation et élimination continues des vulnérabilités	Oui	CS14	Accès contrôlé en fonction du besoin de savoir	Oui
CS5	Utilisation contrôlée des privilèges d'administration	Oui	CS15	Contrôle d'accès sans fil	Oui
CS6	Maintenance, surveillance et analyse des journaux d'audit	Oui	CS16	Surveillance et contrôle des comptes	Oui
CS7	Protections des e-mails et des navigateurs Web	Oui	CS17	Évaluation des compétences en sécurité et formation appropriée pour combler les lacunes	S/O
CS8	Défenses contre les malwares	Oui	CS18	Sécurité des logiciels applicatifs	Oui
CS9	Limitation et contrôle des ports réseau, protocoles et services	Oui	CS19	Réponse aux incidents et gestion	S/O
CS10	Possibilité de récupérer les données	Non	CS20	Tests d'intrusion et exercices « Red Team »	S/O



Franchissez la ligne d'arrivée !



Notre suite Total Security offre des services uniques pour répondre aux critères RGPD spécifiques, notamment :

Threat Detection and Response (TDR) – Le règlement RGPD impose la « sensibilisation situationnelle » que WatchGuard propose avec sa fonction ThreatSync unique. ThreatSync met en corrélation les informations de sécurité des appareils réseau et d'accès pour vous informer des incidents de sécurité croissants dans un tableau de bord simple à interpréter.

De plus, vous pouvez créer des règles pour corriger automatiquement les incidents au « scoring élevé » en plus des mesures « préventives, correctives et d'atténuation en quasi temps réel ». Encore mieux, une fois une menace éliminée, les informations sont partagées avec notre processus d'intelligence sur les menaces pour permettre de l'identifier et empêcher toute nouvelle occurrence sur le réseau ! Et dans la mesure où TDR est un service basé dans le Cloud, vous pouvez décider de conserver vos données dans l'UE conformément à l'article du règlement sur le transfert des données.

Un score de menace unique et complet permet de réagir immédiatement, en toute confiance

Des informations supplémentaires offrent davantage de détails sur les signatures ou les flux d'informations sur les menaces qui ont été exploités

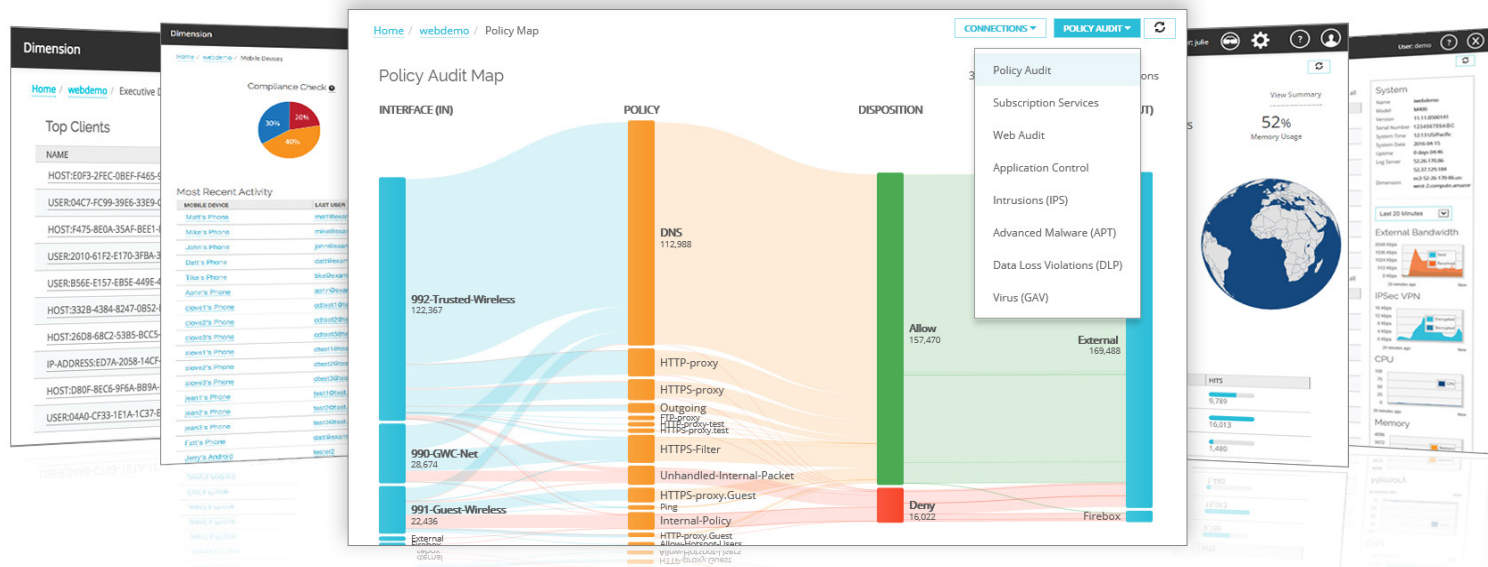
Évaluez votre niveau de risque global en collectant et en analysant les données provenant de votre appliance Firebox et des agents Host Sensor

Threat Detection and Response



WatchGuard Dimension™ – Pour satisfaire les exigences RGPD relatives à l'accès instantané aux journaux de données et rapports démontrant la conformité, Dimension offre une solution rapide et efficace. Le service propose de puissants outils de visibilité et de génération de rapports qui permettent d'identifier et de consolider de manière unique les problèmes et tendances de sécurité majeurs, accélérant ainsi la capacité à combattre les menaces, à établir des rapports sur toutes les activités de sécurité du réseau et à définir des stratégies de sécurité efficaces sur l'ensemble du réseau.

De plus, Dimension inclut une puissante fonction d'anonymisation des données utilisateurs qui consiste à remplacer les informations permettant une identification personnelle présentes dans les rapports, les tableaux de bord et les pages de synthèse de Dimension par des champs de texte codé. Elle code les noms d'utilisateurs, les adresses IP, les noms d'hôtes et les noms des périphériques mobiles à l'aide de séquences alphanumériques uniques générées de manière aléatoire afin de garantir que les données en transit sont masquées.



WatchGuard Dimension



Franchissez la ligne d'arrivée !

Data Loss Prevention (DLP, Prévention des fuites de données accidentelles) : Le règlement RGPD vise à protéger les données et notre service DLP prévient les violations de données accidentelles en identifiant les fichiers de données personnelles et en les empêchant de quitter le réseau. Il recherche les informations personnelles, telles que les numéros de sécurité sociale, les coordonnées bancaires et les dossiers médicaux, en fonction de règles que vous définissez.

Chiffrement et VPN – Chiffrer les données personnelles inactives et en transit est essentiel à la réussite de la mise en conformité, car cela réduit considérablement les opérations de notification en cas de violation de données. Les solutions de sécurité Firebox de WatchGuard permettent la création de VPN par glisser-déposer entre les succursales et le siège. En plus d'être simples et rapides à configurer, ces VPN sont reconnus pour leur stabilité.

Avec les fonctions de sécurité renforcée et de VPN, la visibilité et l'anonymisation des données utilisateur de Dimension, associées à la sensibilisation situationnelle et à l'élimination automatique de Threat Detection and Response, la suite Total Security de WatchGuard est l'équipier idéal pour gagner la course à la conformité RGPD !



Suite Total Security de WatchGuard

SERVICES DE SÉCURITÉ ESSENTIELS



SERVICE DE PRÉVENTION
D'INTRUSIONS (IPS)



AUTORITÉ DE RÉPUTATION
(REPUTATION ENABLED
DEFENSE, RED)



SPAMBLOCKER
(ANTISPAM)



GATEWAY
ANTIVIRUS (GAV, ANTIVIRUS
DE PASSERELLE)



WEBBLOCKER
(FILTRAGE D'URL)



NETWORK DISCOVERY
(DÉCOUVERTE RÉSEAU)



CONTRÔLE
D'APPLICATION

SERVICES DE SÉCURITÉ AVANCÉS



APT BLOCKER –
PROTECTION CONTRE
LES MALWARES AVANCÉS



DATA LOSS PREVENTION
(DLP, PRÉVENTION DES
FUITES DE DONNÉES
ACCIDENTELLES)



THREAT DETECTION
AND RESPONSE



DIMENSION
COMMAND



Checklist de la planification RGPD

Notre Checklist de la planification RGPD vous aide à commencer l'évaluation et la mise en œuvre des mesures de conformité RGPD. Cette ressource ne constitue pas une liste exhaustive des critères et doit être utilisée avec d'autres ressources pour élaborer un plan de conformité complet.

☒ **Identifiez les champs de données personnelles que vous collectez sur les citoyens de l'UE.**

- Quelles sont les données personnelles collectées et/ou traitées ?
- Où sont-elles stockées ou transmises ? Pendant combien de temps ?
- Quels processus et stratégies de conservation régissent ces données ? Peuvent-ils être réduits ?
- Cette collecte est-elle gérée en interne ou en externe ?
- Ces données restent-elles en permanence dans l'UE ?

☒ **Définissez les informations et processus de consentement appliqués lors de la collecte de ces données.**

- Le consentement explicite est-il demandé de façon claire aux personnes concernées avant de collecter et de traiter leurs données ?
- Le consentement est-il obtenu au moment de la collecte ?
- La demande de consentement identifie-t-elle le responsable du traitement, le sous-traitant et le Délégué à la protection des données, et contient-elle leurs coordonnées de contact, le cas échéant ?
- Décrit-elle l'objet du traitement, la sécurité du traitement, ainsi que son cadre légal ?
- Indique-t-elle la durée pendant laquelle les données seront stockées ?
- Nomme-t-elle les destinataires ou la catégorie des destinataires des données ?
- Explique-t-elle à la personne concernée son droit d'accès, de rectification, de demande d'effacement ou de portabilité de ses données, ainsi que son droit de réclamation auprès d'une autorité de contrôle ?
- Stipule-t-elle l'intention de transférer les données en dehors de l'UE ?
- Stipule-t-elle si la collecte des données est obligatoire ou facultative, ainsi que les conséquences de la non-fourniture desdites données ?
- Est-il aussi facile de retirer son consentement que de le donner ?

☒ **Définissez le mode de communication avec les personnes concernées par les données.**

- Comment les personnes concernées peuvent-elles accéder, rectifier, faire effacer et extraire leurs données pour transfert ?
- Comment les personnes concernées peuvent-elles retirer leur consentement ?
- Comment l'entreprise contacte-t-elle les personnes concernées pour signaler un incident ?

☒ **Déterminez si les mesures liées à la tenue de registres et les stratégies de traitement des données actuelles sont adaptées.**

- Les réponses aux demandes de consentement faites aux personnes concernées sont-elles conservées ?
- Les événements sur le traitement des données personnelles sont-ils conservés ou consignés ?
- Ces données sont-elles sécurisées et peuvent-elles faire l'objet de requêtes, recherches ou rapports par des personnes autorisées ?
- Les règles régissant le mode de traitement des données sont-elles actualisées conformément au Règlement ?
- Si un responsable du traitement réside en dehors de l'UE, un représentant est-il désigné au sein de l'UE et cette information est-elle consignée ?
- Si vous faites appel à des services de traitement externes, l'accord légal inclut-il les clauses nécessaires pour garantir la sécurité et le traitement appropriés des données personnelles conformément au RGPD ?
- Un contrôle d'accès aux serveurs et bâtiments suffisant est-il mis en œuvre pour empêcher toute personne non autorisée d'accéder aux données personnelles ?

☒ **Déterminez si les pratiques et technologies liées à la sécurité des données respectent les exigences RGPD.**

- Des mesures techniques et opérationnelles sont-elles appliquées pour garantir la protection des données contre la destruction accidentelle ou illégale, la perte ou l'altération, mais aussi contre la conservation, le traitement, l'accès et la divulgation non autorisés ou illégaux ?
- La stratégie de sécurité couvre-t-elle les points suivants ?
 - Comment protéger les données pendant leur stockage et leur transmission ?
 - Comment restaurer l'accès aux données en cas d'incident affectant la disponibilité ?
 - Comment garantir la sensibilisation situationnelle aux risques et permettre l'application de mesures préventives, correctives et d'atténuation en quasi temps réel en cas de détection de vulnérabilités ou d'incidents présentant un risque pour les données ?
 - Description du processus d'évaluation régulière de l'efficacité des stratégies de sécurité
- Existe-t-il un processus de notification des violations dans les 72 heures ?
- Une analyse d'impact relative à la protection des données a-t-elle été réalisée pour déterminer si les opérations de traitement sont susceptibles de présenter des risques spécifiques ? A-t-elle été réalisée au cours des deux dernières années ou immédiatement après l'apparition de nouveaux risques spécifiques aux opérations de traitement ?
- Un Délégué à la protection des données a-t-il été désigné ?

Les réponses aux questions de cette checklist vous aideront à identifier vos éventuelles lacunes pour les combler dans les délais.





Pour en savoir plus, rendez-vous sur www.watchguard.com

**Siège social mondial
États-Unis**

Tél : +1.206.613.6600

E-mail : sales@watchguard.com

Bureaux français

Tél : +33 (0)1 40 90 30 35

E-mail : france@watchguard.com

**Siège social APAC et SEA
Singapour**

Tél : +65.6536.7717

E-mail : inquiry.sea@watchguard.com



1. <http://www.eugdpr.org/>
2. https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
3. <https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf>

Limite de garanties : Les informations contenues dans ce document sont fournies « en l'état » sans aucune représentation ou garantie, qu'elle soit expresse ou implicite. Assistance professionnelle : Vous ne devez pas substituer les informations de ce document à des conseils juridiques. Pour toute question spécifique d'ordre juridique, demandez conseil à votre avocat ou tout autre professionnel du service juridique.

© 2017 WatchGuard Technologies, Inc. Tous droits réservés. WatchGuard, le logo WatchGuard et Firebox sont des marques déposées de WatchGuard Technologies, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales appartiennent à leurs détenteurs respectifs. Référence : WGCE66998_062617