CHUBB®

# Règlement général sur la protection des données (RGPD) de l'Union européenne

## Ce qu'il faut savoir sur le RGPD : Un guide pour les entreprises nord-américaines

## Comment Chubb peut vous aider à réduire vos cyberrisques

CHUBB®

# Ce qu'il faut savoir sur le RGPD

Le nouveau RGPD vise à établir un ensemble unique de règles dans toute l'Union européenne. Obligatoire, il harmonise les lois nationales sur la protection des données et couvre les changements technologiques et sociaux des deux dernières décennies.

Il vise à garantir que les entreprises qui détiennent des données personnelles de citoyens de l'UE soient responsables et redevables de ces données, quel que soit l'endroit du globe où elles se trouvent.

## Le champ d'application du Règlement comprend, entre autres, les éléments suivants :

**Consentement** au traitement des données personnelles et consentement explicite au traitement de catégories particulières de données (par exemple, les données relatives à la santé).

**Notification en temps utile** des violations de données aux autorités de protection des données et aux personnes concernées, sans retard injustifié.

Date d'entrée en vigueur : **25 mai 2018**

Droit **à l'effacement** et **à l'oubli.**

Accent supplémentaire sur la responsabilité des **sous-traitants de données** par rapport aux responsables du traitement des données.

**RGPD**

Nécessité de réaliser des **évaluations des incidences** sur la protection des données dans le cadre d'activités de traitement à haut risque.

- Le responsable du traitement des données :
  Au sens large, il s'agit de la personne, de l'entreprise ou de l'organisme qui « détermine les finalités et les moyens » du traitement des données.
- Le sous-traitant des données : Au sens large, il s'agit de la personne, de l'entreprise ou de l'organisme qui traite les données personnelles pour le compte du responsable du traitement.

Droit à la **portabilité des données**

Nouvelles sanctions : **amendes** jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial, **avertissements** de la part des autorités de protection des données et **audits**.

> Comment Chubb peut vous aider à réduire vos cyberrisques

# Ce qu'il faut savoir sur le RGPD

## Article 32 : Sécurité du traitement – Le Règlement modifie fondamentalement le droit européen en matière de protection de la vie privée

L'Union européenne a toujours disposé d'un certain nombre de règlements en matière de protection de la vie privée auxquelles elle doit se conformer. Le RGPD n'a pas seulement étoffé ces principes de confidentialité déjà établis, mais a ajouté un nouvel élément de sécurité pour créer une obligation de protection axée sur le traitement sécurisé des données et sur le risque lié à leur divulgation. En réalité, la législation n'exige pas la perte réelle ou la divulgation non autorisée de données pour qu'une amende soit imposée. Des amendes peuvent être infligées si une enquête sur une infraction présumée ou un audit de procédure effectué par une autorité de protection des données comme l'Information Commissioner's Office (ICO) démontre que les exigences du Règlement n'ont pas été respectées.

Les exigences du Règlement sont fondées sur le risque plutôt que sur la prescription.

Il incombe clairement aux responsables du traitement des données et aux sous-traitants de mettre en œuvre des « mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. » Il convient de noter que la double responsabilité couvre également les mesures organisationnelles (politique, procédure, formation, etc.) et la protection technologique.

Certaines clauses de l'article 32 précisent les exigences relatives aux « mesures » de sécurité à prendre pour éviter les risques.

### 1. Chiffrement

La formulation de la clause suggère que tant le responsable du traitement que le sous-traitant doivent assurer un niveau de sécurité approprié au risque, à savoir, entre autres, le chiffrement des données. Dans le cadre des activités de traitement à haut risque, les responsables du traitement doivent s'assurer qu'une évaluation des risques est entreprise, notamment une évaluation des mesures de sécurité comme le chiffrement.

### 2. Systèmes et services de traitement

Les obligations dépassent désormais la protection des données pour inclure l'infrastructure. Les sous-traitants doivent désormais fournir aux responsables du traitement des garanties suffisantes pour mettre en œuvre les mesures techniques et organisationnelles appropriées. En d'autres termes, les sous-traitants doivent s'assurer que leur infrastructure, leur équipement et le flux de leur information sont continuellement accessibles et que la prestation de services est maintenue.

Des menaces comme les attaques DDoS et les rançongiciels peuvent provoquer une interruption du service. L'indisponibilité de données personnelles est désormais considérée comme une violation susceptible de déclencher des sanctions semblables à la perte ou à la divulgation non autorisée de données.

Les responsables du traitement des données devront s'assurer que leur sécurité est suffisamment robuste pour garantir une protection contre ce type de menace. Il s'agira notamment de procéder à une évaluation appropriée des risques et des contrôles actuels.

> Comment Chubb peut vous aider à réduire vos cyberrisques

# Ce qu'il faut savoir sur le RGPD

### 3. Rétablir la disponibilité des données personnelles et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique

Des phrases clés sont incluses dans cette section du Règlement. L'expression **Rétablir** introduit le besoin de résilience du système et éventuellement la mise à disposition d'un site de secours pour assurer la continuité du service.

L'utilisation de l'expression « **dans les délais appropriés** » suggère qu'il est important que le responsable du traitement envisage toutes les conséquences possibles d'une violation. Il conviendrait de prendre en considération les conséquences sur les particuliers ainsi que les besoins éventuels des consommateurs et des particuliers qui accèdent à des données autres que pour des besoins commerciaux.

En mentionnant à la fois un incident physique et un incident technique, la responsabilité s'étend au-delà des cyberattaques et englobe les incendies, les inondations, les pannes et d'autres risques habituels. Et ces considérations doivent

### 4. Test et évaluation des mesures techniques et organisationnelles

Cette partie du Règlement suggère que l'évaluation des risques est nécessaire pour établir le besoin des mesures et confirmer leur efficacité au moyen de tests.

## Résumé

Les exigences du RGPD dépassent la protection des données personnelles :

- Évaluation des risques au-delà de l'évaluation des incidences sur la vie privée
- Nécessité de garantir un niveau de sécurité adapté au risque, à savoir, entre autres, le chiffrement des données
- Redondance et résilience des systèmes désormais obligatoire
- Planification de la reprise après sinistre avec prise en compte de l'élément « délai »
- Test et évaluation continue de toutes les mesures de sécurité, tant organisationnelles que techniques

> Comment Chubb peut vous aider à réduire vos cyberrisques

# Comment Chubb peut vous aider à réduire vos cyberrisques

# Comment Chubb peut vous aider à réduire vos cyberrisques

## À qui s’adresse l’assurance Gestion des cyberrisques d’entreprise de Chubb?

La Gestion des cyberrisques d’entreprise (GCE) de Chubb peut aider les organisations de toute taille à se protéger contre une gamme de cyberincidents.

## Comment fonctionne la couverture GCE?

La couverture GCE de Chubb utilise une approche à trois volets pour aider à protéger les organisations contre les pertes dues aux violations de données, à la corruption de données, aux attaques de rançongiciels et à d’autres cyberrisques. Les trois piliers de notre approche sont les suivants :

**1. Atténuation des risques :** Nous fournissons aux assurés l’accès aux outils et aux ressources nécessaires pour aborder et évaluer les points clés des cyberrisques avant qu’un incident ne survienne.

**2. Transfert du risque :** Grâce à notre service de traitement des réclamations de premier ordre, nous sommes aux côtés de nos assurés lors d’un cyberincident et nous portons le fardeau du risque lorsque nous le pouvons.

**3. Services d’intervention en cas d’incident :** Nous collaborons avec une équipe formée d’experts dans plusieurs domaines : juridique, informatique judiciaire, notification, centre d’appel, relations publiques, consultation en matière de fraude, surveillance du crédit et restauration de l’identité pour limiter le risque de perte à la suite d’un cyberincident.

### Couvertures proposées

L’assurance GCE propose des options pour traiter à la fois la couverture de la responsabilité civile des tiers et la couverture de la partie principale. Nous aidons les assurés potentiels à prendre en compte et à traiter les risques en augmentation liés à la cybercriminalité et à la confidentialité des données auxquels toutes les entreprises sont aujourd’hui confrontées.

La **couverture de la responsabilité des tiers** protège l’assuré contre la responsabilité civile résultant de la perte de renseignements confidentiels de tiers, qu’il s’agisse de renseignements personnels ou de renseignements confidentiels de l’entreprise.

La **couverture de la partie principale** vise à limiter les conséquences d’un cyberincident sur les assurés et à leur fournir un certain niveau de protection.

## Pourquoi choisir Chubb?

Chubb est un chef de file mondial de l’assurance contre les cyberrisques depuis 1998 et a contribué à aviser plus de 500 millions de particuliers d’une atteinte à leur vie privée. Cette couverture de premier ordre bénéficie de la solidité financière de Chubb et de sa cote A++. Notre approche globale envers la cyberassurance et notre analyse minutieuse des données exclusives nous permettent de mettre en place une couverture qui protège votre entreprise dans son intégralité.

> En savoir plus sur l’assurance GCE de Chubb

## Nous joindre

Visitez le site www.chubb.com/ca-fr/ pour en savoir plus sur les offres de Chubb et communiquer avec votre souscripteur local.

Chubb. Insured.℠



14-01-1285
(Éd. 07/18)