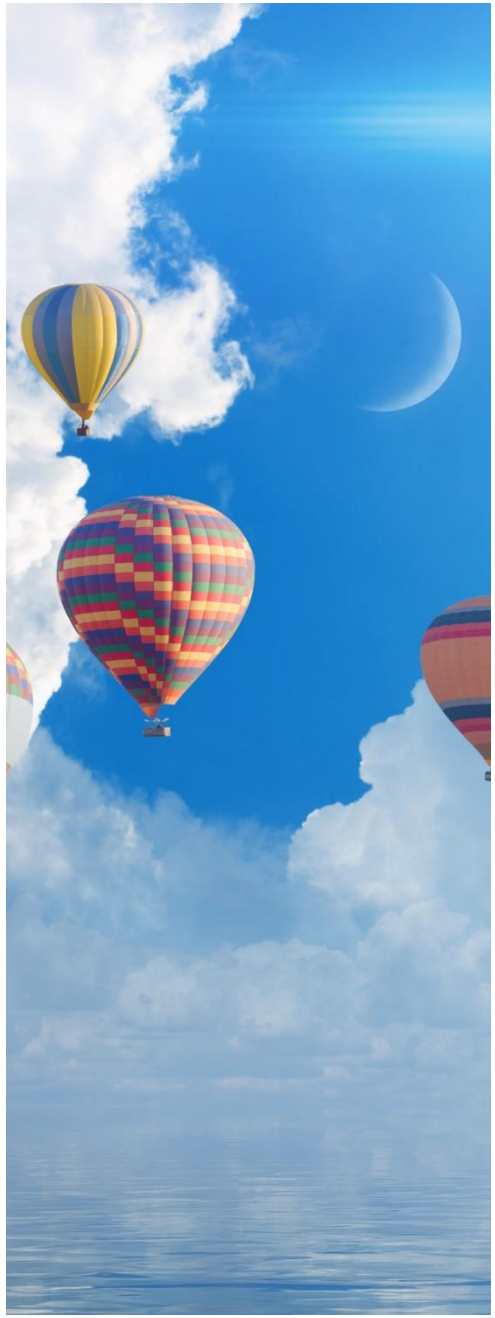
racine
AVOCATS

Cyber attaque

Victime ou coupable



Racine, le Cabinet

Une culture unique

Proche de ses clients, Racine se positionne comme un partenaire.

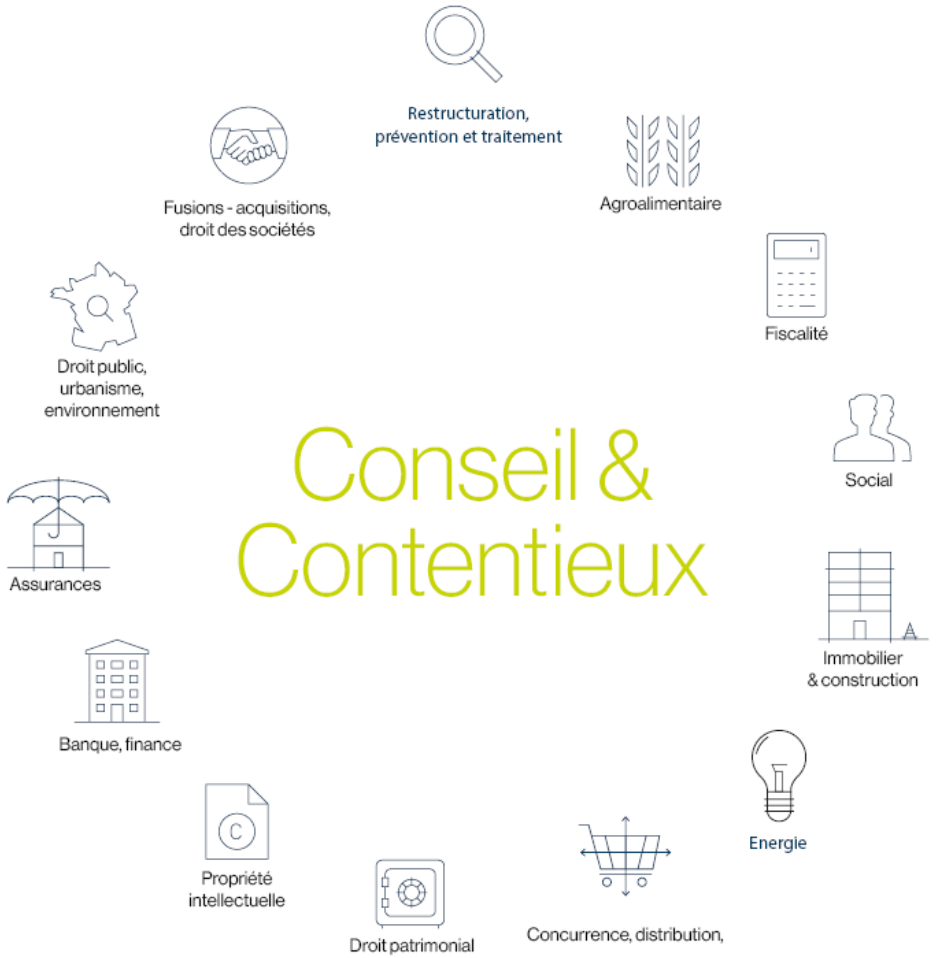
Sa forte technicité juridique lui permet de leur apporter des solutions concrètes et opérationnelles ; sa pratique transverse du contentieux lui confère une réelle capacité d'anticipation.

Le contentieux, exercé par l'ensemble des avocats, fait partie de l'ADN de Racine depuis sa création et représente 50% de son activité.

La culture du cabinet transparait dans son organisation, pensée pour créer des interactions naturelles entre ses départements. Cette transversalité est un atout majeur pour la gestion des dossiers complexes ou pluridisciplinaires.

Les associés sont engagés personnellement dans chaque dossier, de la définition des lignes stratégiques à la résolution complète des problématiques, et en contrôlent le suivi opérationnel.

Enfin, le maillage du territoire national et la capacité de projection internationale de Racine assurent sa capacité d'intervention quel que soit le lieu où ses clients sont implantés.



A propos de nous












Votre interlocuteur

Eric Barbry,

Avocat associé, équipe IP/IT & Data

ebarbry@racine.eu

06 13 28 91 28

Vous pouvez aussi me retrouver sur les réseaux sociaux

www.linkedin.com/in/eric-barbry

Articles et livres blancs

Expert en cyber depuis 2000

Audit de conformité

Mise en conformité

Accompagnement certification

Contrats cyber

Assurance cyber

Formation / sensibilisation

Chartes informatique et autres

Simulations

Violation et gestion de crise

Notification

Accompagnement contrôle AC

racine
AVOCATS

PARTIE 1

Cyber attaque, vous êtes une victime

Victimes en termes de système informatique

Article 323-1

Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende.

Article 323-2

Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende.

Article 323-3

Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende.

Il n’y a pas que les STAD dans la vie

Article 226-4-1

Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende.

Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.

Lorsqu'ils sont commis par le conjoint ou le concubin de la victime ou par le partenaire lié à la victime par un pacte civil de solidarité, ces faits sont punis de deux ans d'emprisonnement et de 30 000 euros d'amende

Il y a aussi les données personnelles

Art. 226-18

Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Code pénal (Partie Législative)

Section 5 - Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques

Art. 226-16

Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 3° du III de l'article 20 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Art. 226-16-1

Le fait, hors les cas où le traitement a été autorisé dans les conditions prévues par la loi n° 78-17 du 6 janvier 1978 précitée, de procéder ou faire procéder à un traitement de données à caractère personnel incluant parmi les données sur lesquelles il porte le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Art. 226-17

Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites aux articles 24, 25, 30 et 32 du règlement (UE) 2016/679 du 27 avril 2016

https://www.cnil.fr/fr/les-sanctions-penales#:~:text=Le%20fait%20de%20collecter%20des,300%20000%20euros%20d'amende.

Victime, coté secret d’affaires

Article L151-1

Créé par LOI n° 2018-670 du 30 juillet 2018 - art. 1

Est protégée au titre du secret des affaires toute information répondant aux critères suivants :

1° Elle n'est pas, en elle-même ou dans la configuration et l'assemblage exacts de ses éléments, généralement connue ou aisément accessible pour les personnes familières de ce type d'informations en raison de leur secteur d'activité ;

2° Elle revêt une valeur commerciale, effective ou potentielle, du fait de son caractère secret ;

3° Elle fait l'objet de la part de son détenteur légitime de mesures de protection raisonnables, compte tenu des circonstances, pour en conserver le caractère secret.

Article L152-1

Créé par LOI n° 2018-670 du 30 juillet 2018 - art. 1

Toute atteinte au secret des affaires telle que prévue aux articles L. 151-4 à L. 151-6 engage la responsabilité civile de son auteur.

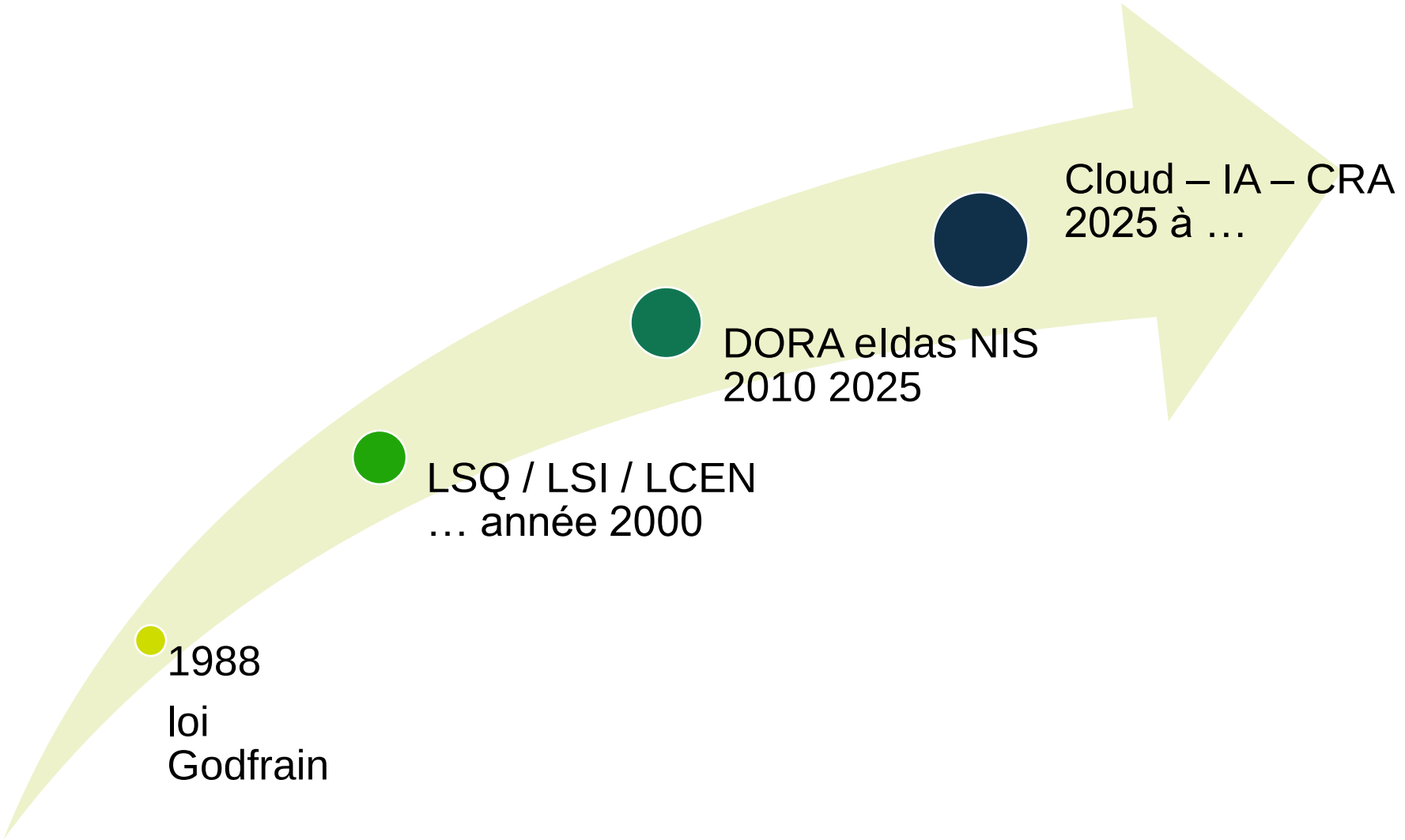
racine
AVOCATS

PARTIE 2

Cyber attaque, et si vous étiez coupable

PEUT ON ETRE VICTIME ET COUPABLE ?

EVOLUTION DU CADRE LEGISLATIF


Cloud – IA – CRA
2025 à …
DORA eIdas NIS
2010 2025
LSQ / LSI / LCEN
… année 2000
1988
loi
Godfrain

Référentiel légal

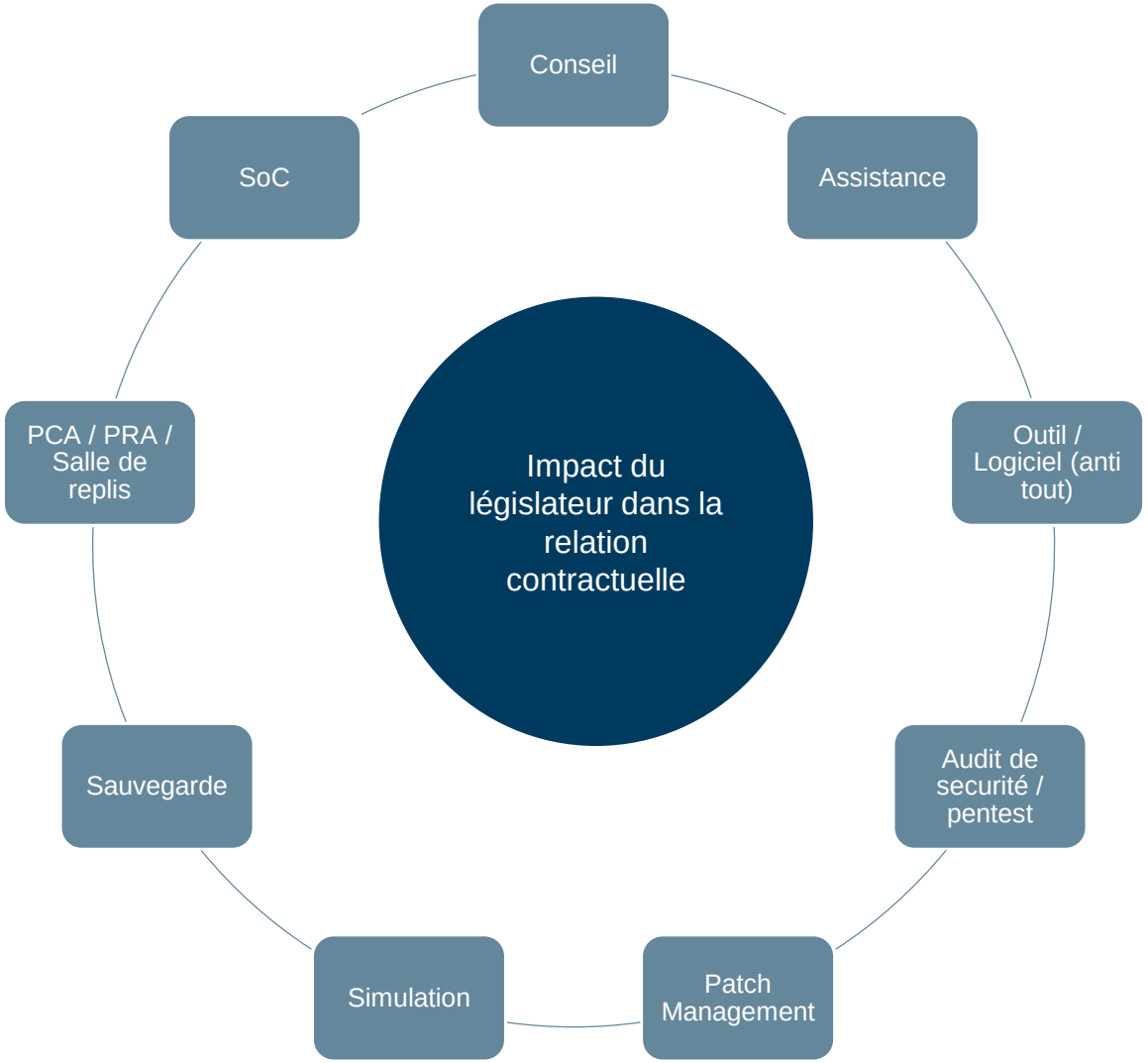
Code – Pénal / Sécurité intérieur / défense / autre

Textes européens :

- Règlement : RGPD/DORA/eIdas 2
- Directives : NIS 2
- Mixte : NIS 2

Loi : France / EU / Monde

Référentiel contractuel



Référentiel normatif

Numéro	Objet
ISO/IEC 27001	Système de management de la sécurité de l'information (SMSI) - Exigences.
ISO/IEC 27002	Code de bonnes pratiques pour les mesures de sécurité de l'information.
ISO/IEC 27003	Lignes directrices pour la mise en œuvre d'un SMSI.
ISO/IEC 27004	Mesures pour l'évaluation de la performance du SMSI.
ISO/IEC 27005	Gestion des risques liés à la sécurité de l'information.
ISO/IEC 27006	Exigences pour les organismes de certification du SMSI.
ISO/IEC 27007	Lignes directrices pour l'audit des SMSI.
ISO/IEC 27008	Lignes directrices pour l'examen des mesures de sécurité.
ISO/IEC 27009	Application sectorielle des exigences ISO/IEC 27001.
ISO/IEC 27010	Communication intersectorielle pour la sécurité de l'information.
ISO/IEC 27011	Lignes directrices pour le secteur des télécommunications.
ISO/IEC 27013	Intégration des SMSI et des systèmes de management de services IT.
ISO/IEC 27014	Gouvernance de la sécurité de l'information.
ISO/IEC 27015	Lignes directrices pour le secteur financier.

27701 – Données persos

ISO/IEC 27017	Contrôles de sécurité pour les services Cloud.
ISO/IEC 27018	Protection des données personnelles dans le Cloud.
ISO/IEC 27019	Sécurité de l'information pour les secteurs énergétiques.
ISO/IEC 27021	Compétences des professionnels du SMSI.
ISO/IEC 27031	Continuité d'activité relative aux TIC.
ISO/IEC 27032	Cybersécurité et interactions avec la sécurité de l'information.
ISO/IEC 27033	Sécurité des réseaux.
ISO/IEC 27034	Sécurité des applications.
ISO/IEC 27035	Gestion des incidents de sécurité de l'information.
ISO/IEC 27036	Gestion des relations de sécurité avec les tiers.
ISO/IEC 27037	Lignes directrices pour la collecte des preuves numériques.
ISO/IEC 27040	Sécurité des systèmes de stockage.
ISO/IEC 27041	Évaluation des processus de traitement des preuves numériques.
ISO/IEC 27042	Analyse des preuves numériques.
ISO/IEC 27050	Gestion de la découverte électronique (e-Discovery).

Les « bonnes pratiques »

SOMMAIRE

CNIL.
PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles

ANSSI

ACPR
BANQUE DE FRANCE

LES ELEMENTS COMMUNS

Les tendances

Les tendances « connues »

- Les règlements supplantent les directives
- Plus d’engagements
- Plus de sanctions

Les tendances « moins connues »

- Responsabilité des « organes de l’entreprise »
- Relation avec les prestataires IT

Ni obligation de moyen, ni de résultat
Conforme ou non conforme

Organe de direction

Ex DORA

2. L'organe de direction de l'entité financière définit, approuve, supervise et est responsable de la mise en œuvre de toutes les dispositions relatives au cadre de gestion du risque lié aux TIC visé à l'article 6, paragraphe 1.

Aux fins du premier alinéa, l'organe de direction:

a) assume la responsabilité ultime de la gestion du risque lié aux TIC de l'entité financière;

b) met en place des stratégies visant à garantir le maintien de normes élevées en matière de disponibilité, d'authenticité, d'intégrité et de confidentialité des données;

c) définit clairement les rôles et les responsabilités pour toutes les fonctions liées aux TIC et met en place des dispositifs de gouvernance appropriés pour assurer une communication, une coopération et une coordination efficaces et en temps utile entre ces fonctions;

d) assume la responsabilité globale de la définition et de l'approbation de la stratégie de résilience opérationnelle numérique visée à l'article 6, paragraphe 8, y compris la détermination du niveau approprié de tolérance au risque lié aux TIC de l'entité financière, tel que visé à l'article 6, paragraphe 8, point b);

e) approuve, supervise et examine périodiquement la mise en œuvre de la politique de continuité des activités de TIC de l'entité financière et des plans de réponse et de rétablissement des TIC visés, respectivement, à l'article 11, paragraphes 1 et 3, qui peuvent être adoptés en tant que politique spécifique faisant partie intégrante de la politique globale de continuité des activités et du plan de réponse et de rétablissement de l'entité financière;

f) approuve et examine périodiquement les plans internes d'audit des TIC et les audits des TIC de l'entité financière ainsi que les modifications significatives qui y sont apportées;

(Art 5)

30) «organe de direction»: un organe de direction au sens de l'article 4, paragraphe 1, point 36), de la directive 2014/65/UE, de l'article 3, paragraphe 1, point 7), de la directive 2013/36/UE, de l'article 2, paragraphe 1, point s), de la directive 2009/65/CE du Parlement européen et du Conseil (*), de l'article 2, paragraphe 1, point 45), du règlement (UE) nº 909/2014, de l'article 3, paragraphe 1, point 20), du règlement (UE) 2016/1011, et de la disposition pertinente du règlement sur les marchés de crypto-actifs, ou les personnes assimilées qui dirigent effectivement l'entité ou qui exercent des fonctions clés conformément au droit de l'Union ou au droit national applicable;

4. Les membres de l'organe de direction de l'entité financière maintiennent activement à jour des connaissances et des compétences suffisantes pour comprendre et évaluer le risque lié aux TIC et son incidence sur les opérations de l'entité financière, notamment en suivant régulièrement une formation spécifique proportionnée au risque lié aux TIC géré.

(Art 5)

Ex NIS 2

1. Les États membres veillent à ce que les organes de direction des entités essentielles et importantes approuvent les mesures de gestion des risques en matière de cybersécurité prises par ces entités afin de se conformer à l'article 21, supervisent sa mise en œuvre et puissent être tenus responsables de la violation dudit article par ces entités. (Art 20)

2. Les États membres veillent à ce que les membres des organes de direction des entités essentielles et importantes soient tenus de suivre une formation et ils encouragent les entités essentielles et importantes à offrir régulièrement une formation similaire aux membres de leur personnel afin que ceux-ci acquièrent des connaissances et des compétences suffisantes pour déterminer les risques et évaluer les pratiques de gestion des risques en matière de cybersécurité et leur impact sur les services fournis par l'entité. (Art 20)

L’équipe IT en question

5. Les membres de l’encadrement supérieur responsables des TIC rendent compte au moins une fois par an, à l’organe de direction, des constatations visées au paragraphe 3 et formulent des recommandations. (DORA Art 13)

COUPABLE & PREVENTION

Obligation de mettre en œuvre les mesures technique

Article 32

Sécurité du traitement

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins:

a) la pseudonymisation et le chiffrement des données à caractère personnel;

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

2. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

Art. 226-17

Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites aux articles 24, 25, 30 et 32 du règlement (UE) 2016/679 du 27 avril 2016 précité ou au 6° de l'article 4 et aux articles 99 à 101 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Obligation 1 – Sécurisation

Obligation 2 - PCA

Obligation 3 - PRA

Obligation 4 – Audit

Obligation de protection des données

Article 25

Protection des données dès la conception et protection des données par défaut

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.

2. Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.

3. Un mécanisme de certification approuvé en vertu de l'article 42 peut servir d'élément pour démontrer le respect des exigences énoncées aux paragraphes 1 et 2 du présent article.

Minimisation des accès

=

+

Tracabilité

Obligations spécifiques

DORA

NIS 2

PGSSI-S

CRA

RIA

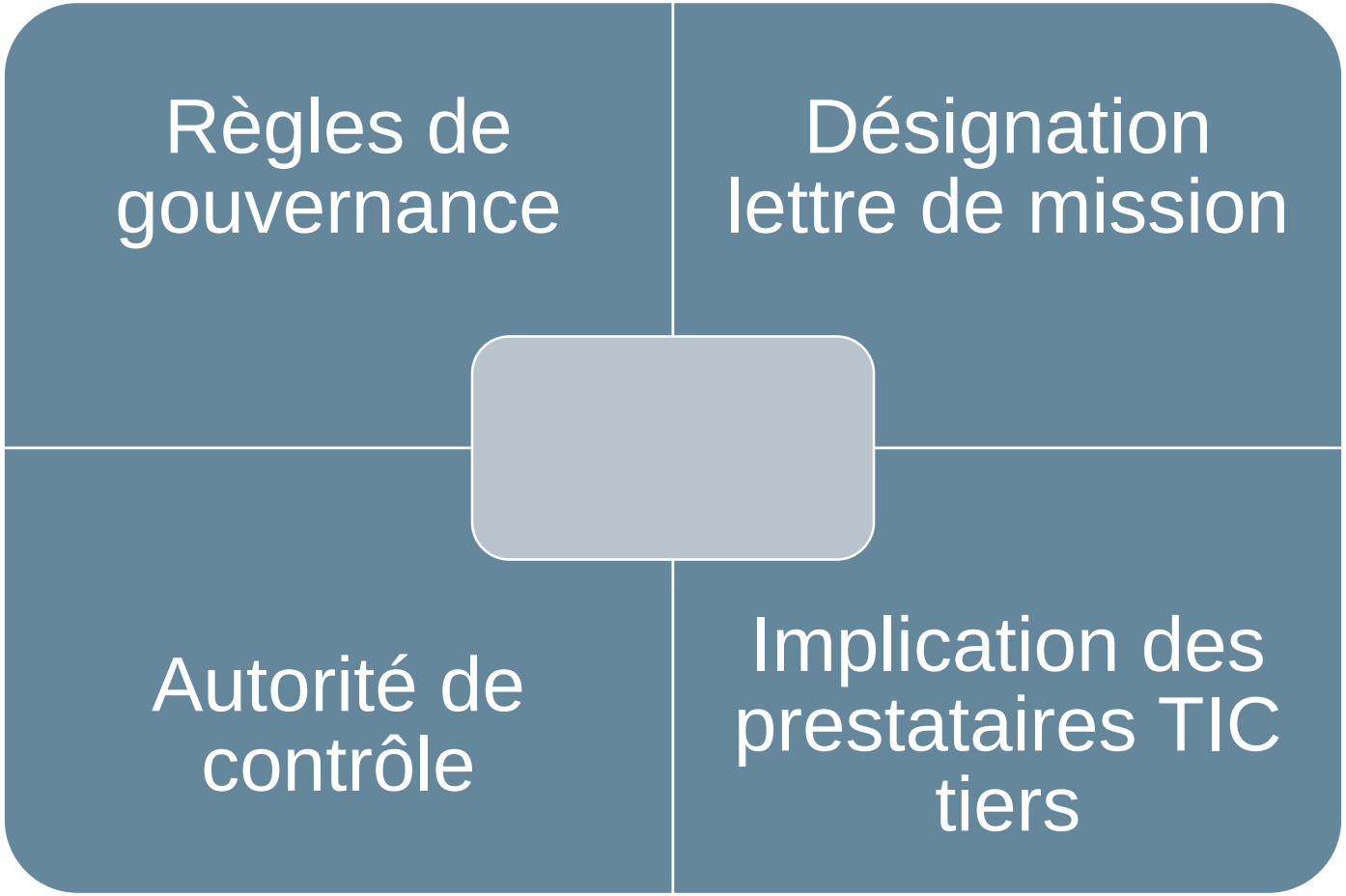
La vision du juge…

Kitetoa c/ Tati CA Paris 30 octobre 2002 - Une entreprise victime d'un accès frauduleux dans un système de traitement automatisé de données "*ne saurait se prévaloir de ses propres carences et négligences pour arguer d'un prétendu préjudice*" en matière de sécurité. Celle-ci est en effet tenue conformément à l'article 226-17 du Code pénal de prendre les précautions utiles, lorsqu'elle procède ou fait procéder à un traitement automatisé d'informations nominatives, pour préserver la sécurité des informations et, notamment, pour empêcher leur communication à des tiers non autorisés

Olivier X / Anses cass 20 mai 2015 Attendu qu'il résulte de l'arrêt attaqué et des pièces de procédure que M. X..., qui s'est introduit sur le site extranet de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail à la suite d'une défaillance technique, s'y est maintenu alors qu'il avait constaté l'existence d'un contrôle d'accès, et a téléchargé des données qu'il a fixées sur différents supports et diffusées à des tiers ; que, poursuivi des chefs d' accès et de maintien frauduleux dans un système de traitement automatisé et de vol de données, il a été relaxé par le tribunal

En dessin c’est plus simple ☺

Les obligations en termes de gouvernance



Information et identification

3. Au plus tard le 17 avril 2025, les États membres établissent une liste des entités essentielles et importantes ainsi que des entités fournissant des services d'enregistrement de noms de domaine. Les États membres réexaminent cette liste et, le cas échéant, la mettent à jour régulièrement et au moins tous les deux ans par la suite.

4. Aux fins de l'établissement de la liste visée au paragraphe 3, les États membres exigent des entités visées audit paragraphe qu'elles communiquent aux autorités compétentes au moins les informations suivantes:

a) le nom de l'entité;

b) l'adresse et les coordonnées actualisées, y compris les adresses électroniques, les plages d'IP et les numéros de téléphone;

c) le cas échéant, le secteur et le sous-secteur concernés visés à l'annexe I ou II; et

d) le cas échéant, une liste des États membres dans lesquels elles fournissent des services relevant du champ d'application de la présente directive.

Les entités visées au paragraphe 3 notifient sans tarder toute modification des informations qu'elles ont communiquées conformément au premier alinéa du présent paragraphe et, en tout état de cause, dans un délai de deux semaines à compter de la date de la modification.

NIS 2 – Article 3

J’ai travaillé avec n’importe qui, n’importe comment

RGPD

- Vérification
- DPA (PAS)
- Audit
- Registre RT

DORA

- Vérification
- Clauses
- Audit
- Registre tiers

NIS 2

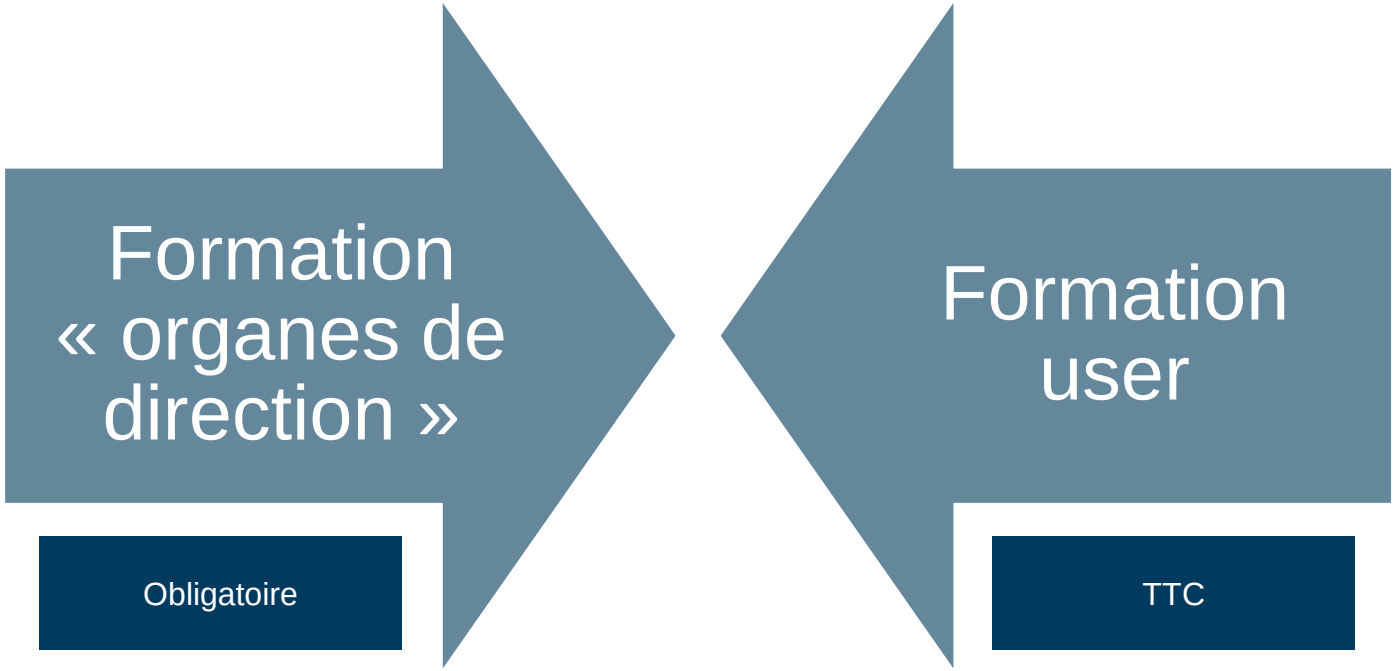
Les mesures visées au paragraphe 1 sont fondées sur une approche «tous risques» qui vise à protéger les réseaux et les systèmes d’information ainsi que leur environnement physique contre les incidents, et elles comprennent au moins: (…)

d) la sécurité de la chaîne d’approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services direct (…°

eIdas 2

- Statut prestataire
- Clauses

Formation



Les États membres veillent à ce que les membres des organes de direction des entités essentielles et importantes soient tenus de suivre une formation et ils encouragent les entités essentielles et importantes à offrir régulièrement une formation similaire aux membres de leur personnel afin que ceux-ci acquièrent des connaissances et des compétences suffisantes pour déterminer les risques et évaluer les pratiques de gestion des risques en matière de cybersécurité et leur impact sur les services fournis par l'entité. (art 20 2 - Gouvernance)

COUPABLE & REACTION

Je n’ai pas notifié

Article 33

Notification à l’autorité de contrôle d’une violation de données à caractère personnel

1. En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l’autorité de contrôle compétente conformément à l’article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d’engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l’autorité de contrôle n’a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

2. Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

3. La notification visée au paragraphe 1 doit, à tout le moins:

Info 1

a) décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d’enregistrements de données à caractère personnel concernés;

b) communiquer le nom et les coordonnées du délégué à la protection des données ou d’un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

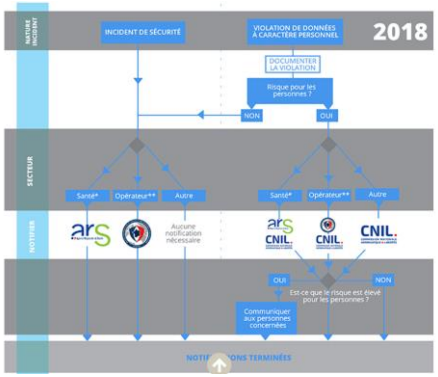
Info 2

c) décrire les conséquences probables de la violation de données à caractère personnel;

Info 3

d) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Je n’ai pas notifié (il n’y a pas que la Cnil dans la vie)



PHAROS
PLATEFORME D'HARMONISATION, D'ANALYSE, DE RECOUPEMENT ET D'ORIENTATION DES SIGNALEMENTS

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

ACPR
BANQUE DE FRANCE

AGENCE DU NUMÉRIQUE EN SANTÉ

ars
Agence Régionale de Santé

HAS
HAUTE AUTORITÉ DE SANTÉ

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

arcep

ANJ
AUTORITÉ NATIONALE DES JEUX

OIV
Organisation Internationale de la Vigne et du Vin

Exemple PSCO eIdas

Article 19

Exigences de sécurité applicables aux prestataires de services de confiance

1. Les prestataires de services de confiance qualifiés et non qualifiés prennent les mesures techniques et organisationnelles adéquates pour gérer les risques liés à la sécurité des services de confiance qu'ils fournissent. Compte tenu des évolutions technologiques les plus récentes, ces mesures garantissent que le niveau de sécurité est proportionné au degré de risque. Des mesures sont notamment prises en vue de prévenir et de limiter les conséquences d'incidents liés à la sécurité et d'informer les parties concernées des effets préjudiciables de tels incidents.

2. Les prestataires de services de confiance qualifiés et non qualifiés notifient, dans les meilleurs délais et en tout état de cause dans un délai de vingt-quatre heures après en avoir eu connaissance, à l'organe de contrôle et, le cas échéant, à d'autres organismes concernés, tels que l'organisme national compétent en matière de sécurité de l'information ou l'autorité chargée de la protection des données, toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ou sur les données à caractère personnel qui y sont conservées.

Le cas échéant, notamment lorsqu'une atteinte à la sécurité ou une perte d'intégrité concerne deux États membres ou plus, l'organe de contrôle notifié informe les organes de contrôle des autres États membres concernés ainsi que l'ENISA.

Exemple santé

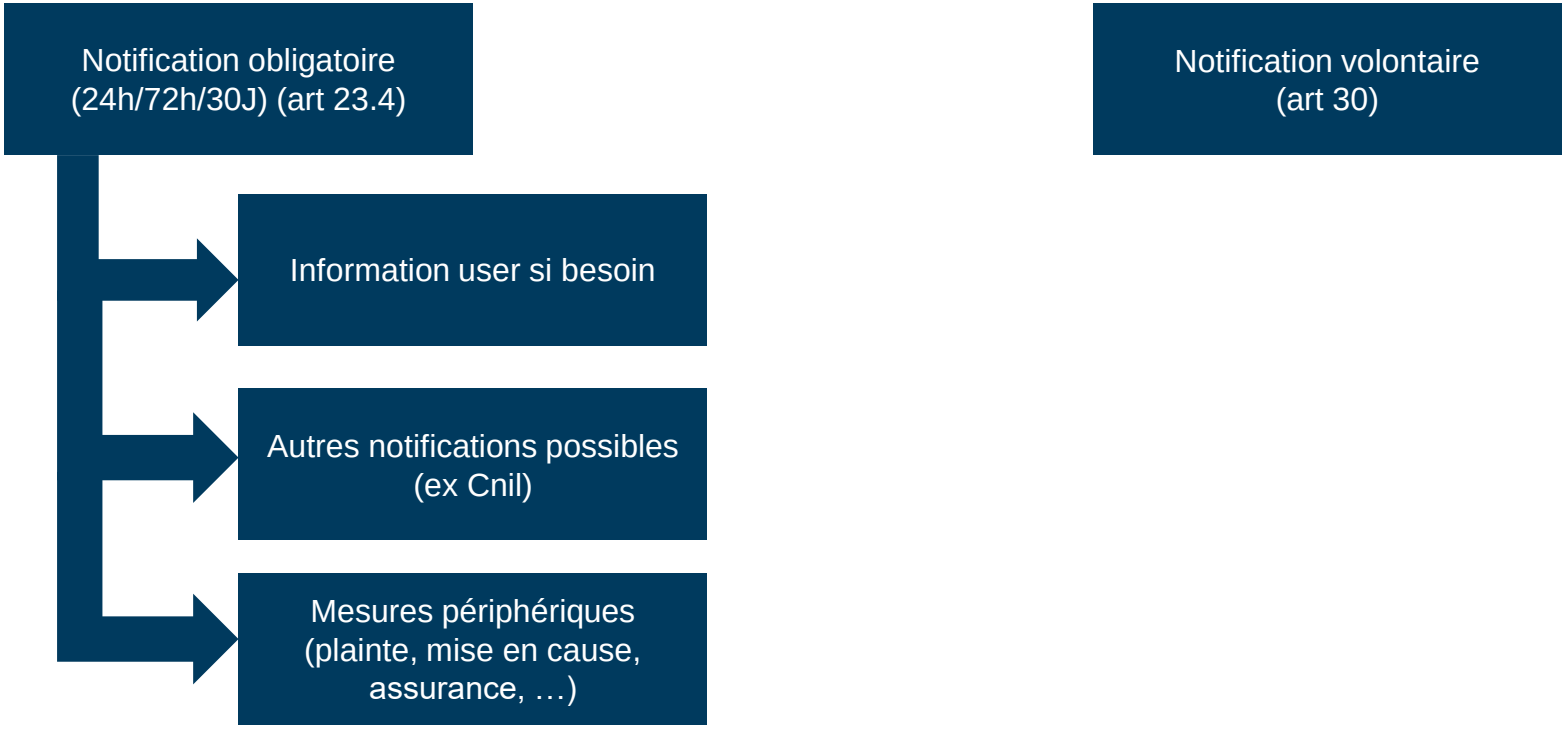
JE DÉCLARE MES INCIDENTS

Depuis le 1er octobre 2017, le Ministère des Solidarités et de la Santé s'est engagé dans la lutte contre les cyberattaques dans le secteur santé, en mettant en place un dispositif de traitement des signalements des incidents de sécurité des systèmes d'information (SSI) des structures de santé. Pour mettre en œuvre cette stratégie nationale de sécurité numérique, il s'appuie sur l'Agence du Numérique en Santé et plus particulièrement sur sa **cellule d'Accompagnement Cyber sécurité des Structures de Santé (ACSS) rebaptisée CERT Santé en avril 2021, après sa reconnaissance en tant que CERT sectoriel pour le domaine de la santé par le CERT-FR.**
Il est indispensable de déclarer ses incidents de sécurité, d'une part pour protéger sa structure mais aussi pour éviter tous risques similaires à une autre structure de santé.

Opérateur de service essentiel (NIS)

RÈGLEMENT (UE) N° 611/2013 DE LA COMMISSION
du 24 juin 2013
concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques

Notifications



Un incident est considéré comme important si:
a) il a causé ou est susceptible de causer une perturbation opérationnelle grave des services ou des pertes financières pour l'entité concernée;
b) il a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables. (art 23) +++ règlement d'execution art 3 à 14)

Je n'ai pas informé (communiqué)

Article 34

Communication à la personne concernée d'une violation de données à caractère personnel

1. Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

Ce qu'il faut dire

2. La communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées à l'article 33, paragraphe 3, points b), c) et d).

3. La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie:

a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement;

b) le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser;

c) elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

4. Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, l'autorité de contrôle peut, après avoir examiné si cette violation de données à caractère personnel est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions visées au paragraphe 3 est remplie.

Je n’ai pas communiqué (il n’y a pas que la Cnil)

Exemple PSCO eldas

Article 19

Exigences de sécurité applicables aux prestataires de services de confiance

1. Les prestataires de services de confiance qualifiés et non qualifiés prennent les mesures techniques et organisationnelles adéquates pour gérer les risques liés à la sécurité des services de confiance qu'ils fournissent. Compte tenu des évolutions technologiques les plus récentes, ces mesures garantissent que le niveau de sécurité est proportionné au degré de risque. Des mesures sont notamment prises en vue de prévenir et de limiter les conséquences d'incidents liés à la sécurité et d'informer les parties concernées des effets préjudiciables de tels incidents.

2. Les prestataires de services de confiance qualifiés et non qualifiés notifient, dans les meilleurs délais et en tout état de cause dans un délai de vingt-quatre heures après en avoir eu connaissance, à l'organe de contrôle et, le cas échéant, à d'autres organismes concernés, tels que l'organisme national compétent en matière de sécurité de l'information ou l'autorité chargée de la protection des données, toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ou sur les données à caractère personnel qui y sont conservées.

Lorsque l'atteinte à la sécurité ou la perte d'intégrité est susceptible de porter préjudice à une personne physique ou morale à laquelle le service de confiance a été fourni, le prestataire de services de confiance notifie aussi, dans les meilleurs délais, à la personne physique ou morale l'atteinte à la sécurité ou la perte d'intégrité.

Je n’ai pas géré la preuve

- Preuve du dommage (assurance/prestataire)
- Preuve du préjudice (assurance/prestataire)
- Preuve des mesures prises (Cnil et autre autorité de contrôle)

Je n’ai pas mis en cause mon prestataire

Je n’ai pas déposé plainte

VOUS ÊTES VICTIME D’UN RANSOMWARE OU DE FISHING ?

Suite à une escroquerie ou une cyberattaque, déposez plainte auprès d’un service de **Police nationale** ou de **Gendarmerie nationale** ou bien adressez un courrier au Procureur de la République auprès du Tribunal de Grande Instance compétent.

Munissez-vous de tous les renseignements suivants :

- Références du (ou des) transfert(s) d'argent effectué(s)
- Références de la (ou des) personne(s) contactée(s): adresse de messagerie ou adresse postale, pseudos utilisés, numéros de téléphone, fax, copie des courriels ou courriers échangés...
- Numéro complet de votre carte bancaire ayant servi au paiement, référence de votre banque et de votre compte, et copie du relevé de compte bancaire où apparaît le débit frauduleux
- Tout autre renseignement pouvant aider à l'identification de l'escroc

Vous pouvez également signaler les faits dont vous avez été victime via la plateforme de signalement « Pharos » ou le numéro dédié : 0811 02 02 17

Des services spécialisés se chargent ensuite de l'enquête :

- **Police nationale :** l’Office central de lutte contre la criminalité liée aux technologies de l’information et de la communication (OCLCTIC) qui dépend de la Sous-direction de lutte contre la cybercriminalité (SDLC)
- **Gendarmerie nationale** : le centre de lutte contre les criminalités numériques (C3N) du Service Central du Renseignement Criminel (SCRC) : cyber@gendarmerie.interieur.gouv.fr
- **Préfecture de police** : la Préfecture de police de Paris, de la Direction centrale du renseignement intérieur (DCRI) et ses équipes de la Brigade d’enquêtes sur les fraudes aux technologies de l’information (BEFTI) compétente uniquement pour Paris et petite couronne (75, 92, 93 et 94) : 01 40 79 67 50

Vous pouvez porter plainte directement auprès du procureur de la République. Il faut envoyer une lettre sur papier libre au tribunal judiciaire du lieu de l'infraction ou du domicile de l'auteur de l'infraction.

La lettre doit préciser les éléments suivants :

- État civil et coordonnées complètes (adresse et numéro de téléphone) du plaignant
- Récit détaillé des faits, date et lieu de l'infraction
- Nom de l'auteur supposé si vous le connaissez (sinon, la plainte sera déposée contre X)
- Noms et adresses des éventuels témoins de l'infraction
- Description et estimation provisoire ou définitive du préjudice
- Documents de preuve : certificats médicaux, arrêts de travail, factures diverses, constats ....
- Volonté de se constituer partie civile

Porter plainte auprès du procureur de la République

Direction de l'information légale et administrative (Dila) - Premier ministre

Accéder au **modèle de document**

Je n’ai pas désigné « rapporté » la situation

5. Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l’autorité de contrôle de vérifier le respect du présent article.

Enfin je n’ai pas été efficace et coopératif

Article 83

Conditions générales pour imposer des amendes administratives

1. Chaque autorité de contrôle veille à ce que les amendes administratives imposées en vertu du présent article pour des violations du présent règlement visées aux paragraphes 4, 5 et 6 soient, dans chaque cas, effectives, proportionnées et dissuasives.

2. Selon les caractéristiques propres à chaque cas, les amendes administratives sont imposées en complément ou à la place des mesures visées à l'article 58, paragraphe 2, points a) à h), et j). Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative, il est dûment tenu compte, dans chaque cas d'espèce, des éléments suivants:

a) la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi;

b) le fait que la violation a été commise délibérément ou par négligence;

c) toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées;

d) le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en vertu des articles 25 et 32;

e) toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant;

f) le degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs;

g) les catégories de données à caractère personnel concernées par la violation;

h) la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation;

i) lorsque des mesures visées à l'article 58, paragraphe 2, ont été précédemment ordonnées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet, le respect de ces mesures;

j) l'application de codes de conduite approuvés en application de l'article 40 ou de mécanismes de certification approuvés en application de l'article 42; et

k) toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation.

Je n’ai pas mentionné la violation dans mon registre

racine
AVOCATS

PARTIE 3

Conclusions

Le plan d’actions

Action 1 – Identifier « votre » référentiel cyber

Action 2 – Dresser la liste des obligations amont / aval

Action 3 – Réaliser un audit de conformité de vos pratiques

Action 4 – Plan d’actions avec règles de priorisation (légale et risque)

Action 5 – Composer une équipe projet avec un sponsor

Merci de votre attention,

à votre disposition pour répondre à vos questions