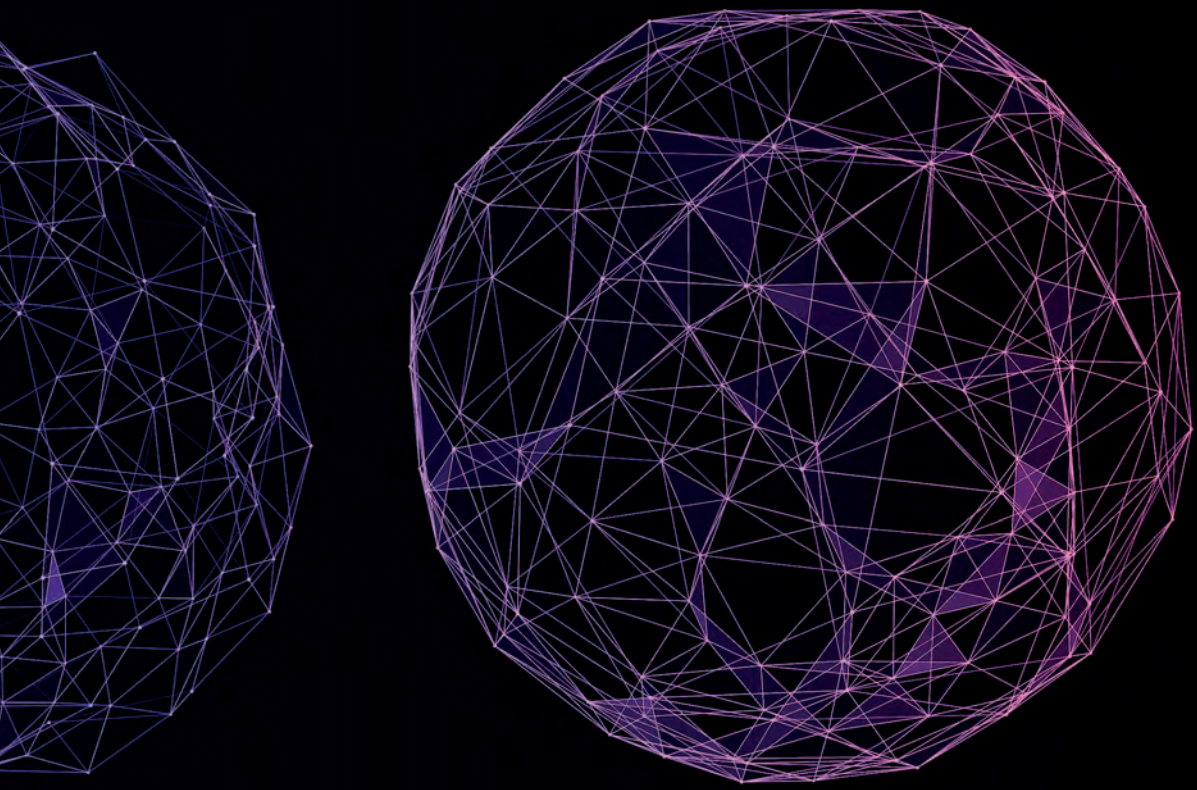
LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Commissariat du gouvernement
à la protection des données
auprès de l'État



PRÉVENTION ET GESTION DES INCIDENTS DE SÉCURITÉ ET DES VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL

PRÉFACE

Léif Lieserinnen a Lieser,

D'Cybersécherheet an de Schutz vu perséinlechen Informatiounen si fundamental fir d'Vertrauen an eis demokratesch Institutiounen. D'Zuel vun de Cyberattacke geet weltwäit kontinuéierlech erop, an och Lëtzebuerg ass vun dësem Phenomen net verschount. D'Regierung ass entschloss, de Geforen, déi vun dësen Aktivitéiten ausginn, entgéint ze wierken. D'Widderstandsfäegkeet vun eisen ëffentlechen Instanzen am Beräich vun der Informatiounssécherheet ass essentiel. D'Biergerinnen a Bierger mussen sech drop verloosse kënnen, datt de Staat an d'Gemengen déi vun hinne veraarbecht Informatioune mat der néideger Virsiicht behandelen.

Jiddwer Eenzelen iwwerhëlt a sengem Aarbechtsalldag eng grouss Verantwortung an dréit duerch säi Verhalen zur Informatiounssécherheet, an domat zum Erhalt vum Vertrauen an eis ëffentlech Instanze bei. Aus dësem Grond leet d'Regierung e grousse Wäert op déi néideg Sensibilisatioun am Beräich vun der Cybersécherheet.

Dës Publikatioun vum Kommissariat fir Dateschutz beim Staat ass an Zesummenaarbecht mat den anere Verwaltungen an Autoritéiten ausgeschafft ginn, déi fir d'Cybersécherheet zoustänneg sinn. Sie enthält gutt Praktiken am Beräich vun der Informatiounssécherheet, déi all Agent soll kennen a respektéieren, an ergänzt déi vill Moossnamen, déi schonns vun dësen Acteuren, wéi och vun Ärer Entitéit geholl goufen. Ech sinn dervun iwwerzeegt, datt dës Publikatioun zur Cybersécherheet-Kultur, an domat zu engem bessere Schutz vun den Informatiounen am ëffentlechen Déngscht bäidroe wäert.

Ech felicitéieren d'Auteure fir hiert Wierk, dat Iech erlabe wäert, d'grondsätzleche Konzepter vun der Cybersécherheet nach besser ze verënnerlechen, a se an Ärem berufflechen Alldag unzewennen.

Ech wënschen Iech eng beräicherend Lektür.

Xavier BETTEL
Premier ministre
Ministre des Communications et des Médias

Cette publication élaborée par le Commissariat du gouvernement à la protection des données auprès de l'Etat (CGPD) est le fruit d'une étroite collaboration entre les acteurs clés impliqués dans la sécurité de l'information, la protection des données à caractère personnel ainsi que la gestion des incidents de sécurité.

Les acteurs ayant participé à l'élaboration de la présente publication sont :

- le Haut-Commissariat à la protection nationale,
- l'Agence nationale de la sécurité des systèmes d'information,
- le Centre de traitement des urgences informatiques (« GOVCERT »),
- le Centre des technologies de l'information de l'Etat,
- la Luxembourg House of Cybersecurity,
- l'Institut luxembourgeois de régulation,
- la Commission nationale pour la protection des données,
- le Centre commun de la sécurité sociale.

TABLE DES MATIÈRES

INTRODUCTION // 9

CHAPITRE 1 //

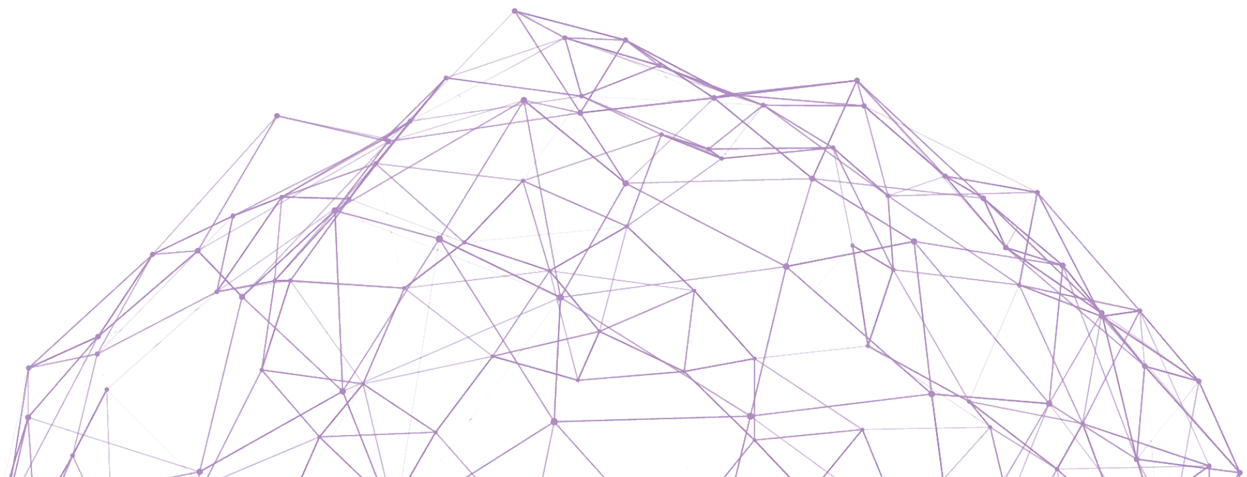
Les entités étatiques compétentes en matière de sécurité de l'information et de protection des données à caractère personnel 15

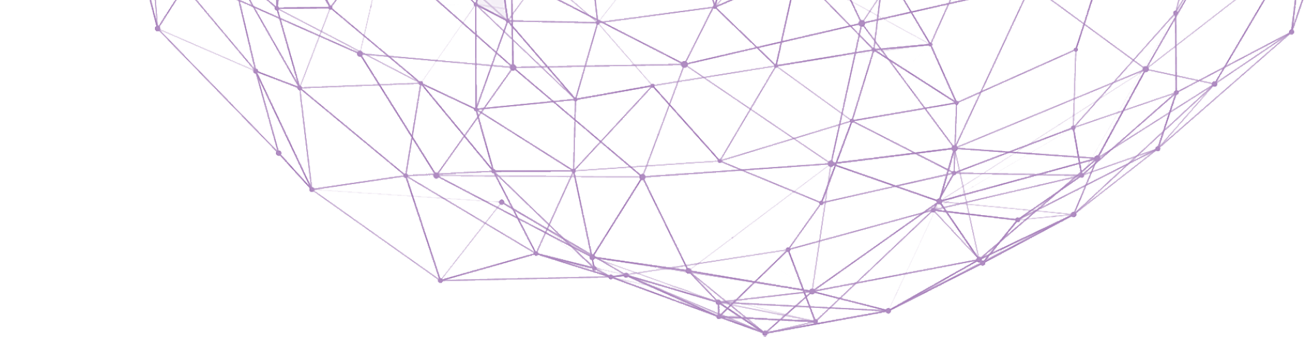
Section 1 : Le Haut-Commissariat à la protection nationale 17
Section 2 : L'Agence nationale de la sécurité des systèmes d'information 18
Section 3 : Le Centre de traitement des urgences informatiques 20
Section 4 : Le Comité interministériel de coordination en matière de cyberprévention et de cybersécurité 21
Section 5 : Le Centre des technologies de l'information de l'Etat 23
Section 6 : La Luxembourg House of Cybersecurity 24
Section 7 : L'Institut luxembourgeois de régulation 25
Section 8 : Le Commissariat du gouvernement à la protection des données auprès de l'Etat 26
Section 9 : La Commission nationale pour la protection des données 27

CHAPITRE 2 //

L'obligation de garantir la sécurité de l'information et des données à caractère personnel 29

Section 1 : Les concepts de sécurité de l'information et de protection des données à caractère personnel 30
Section 2 : L'obligation de garantir la sécurité des données conformément au RGPD 34
Section 3 : L'évaluation des risques et la mise en œuvre de mesures appropriées conformément au RGPD 41
Section 4 : L'agent au centre de la sécurité de l'information et des données 55





CHAPITRE 3 //

La survenance et la détection des incidents de sécurité et des violations de données à caractère personnel 79

Section 1 : Un risque omniprésent 80
Section 2 : Les principaux types d'attaques et causes des incidents de sécurité 82
Section 3 : L'obligation de détecter les incidents de sécurité et les violations de données à caractère personnel 94
Section 4 : Le rôle de l'agent dans la détection des incidents de sécurité 95

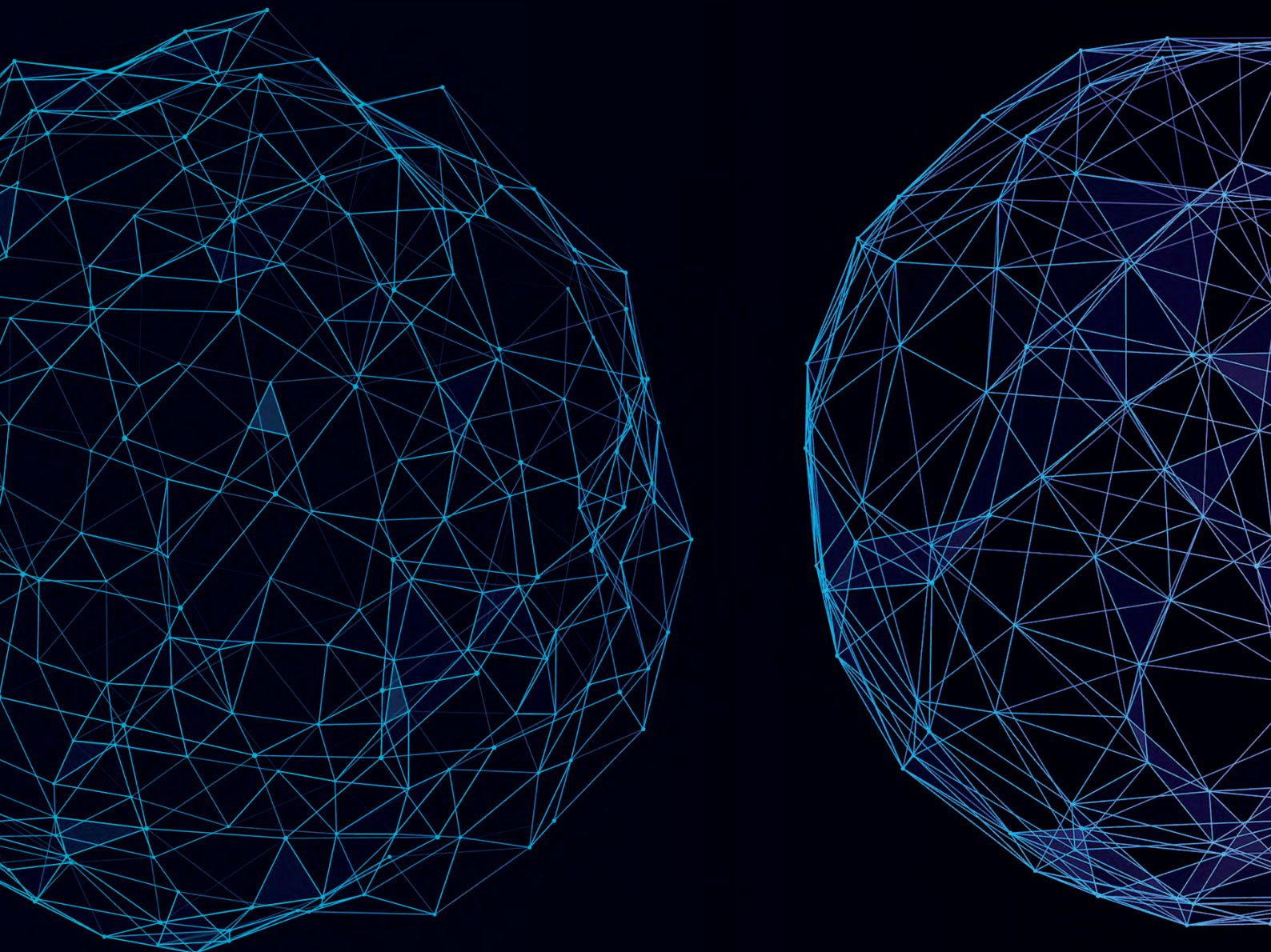
CHAPITRE 4 //

La gestion des « violations de données à caractère personnel » par l'administration conformément au RGPD 101

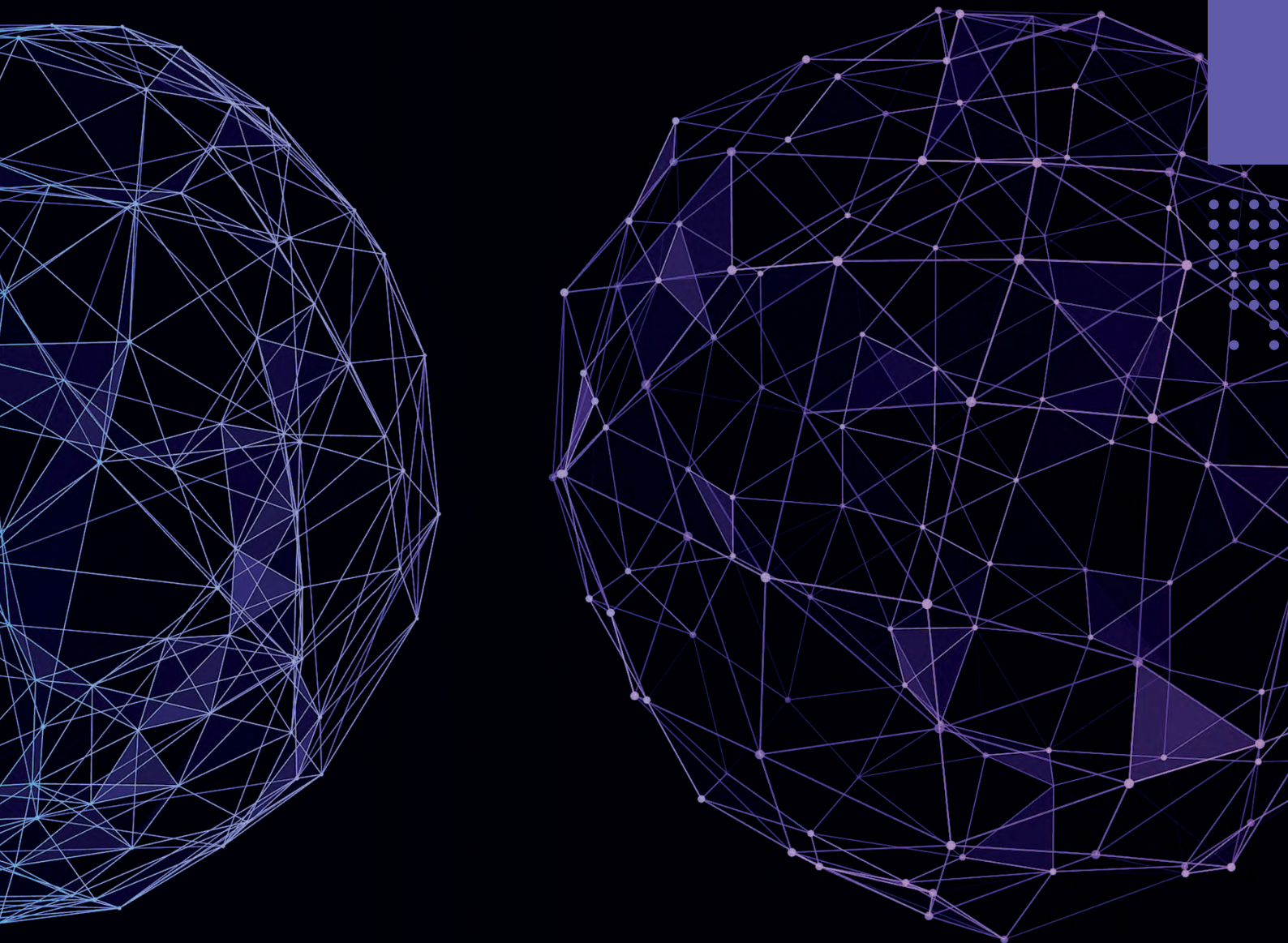
Section 1 : Le concept de « violation de données à caractère personnel » 102
Section 2 : L'administration en charge de la gestion des violations de données 108
Section 3 : Le niveau de « risque » comme facteur déterminant des suites à donner à une violation de données 109
Section 4 : L'évaluation objective du risque 111
Section 5 : La documentation interne de la violation de données 119
Section 6 : La notification de la violation de données à la CNPD 121
Section 7 : La communication de la violation de données à la personne concernée 124
Section 8 : Récapitulatif des étapes à suivre 126

CHAPITRE 5 //

Les autres types de notifications d'incidents de sécurité à effectuer par les administrations 129



INTRODUCTION//



INTRODUCTION //

L'importance de garantir la sécurité de l'information et des données à caractère personnel

La sécurité de l'information constitue un volet essentiel de la protection des infrastructures nationales, des données à caractère personnel et, de manière plus générale, des intérêts nationaux luxembourgeois et européens. Elle est indispensable pour consolider la confiance des citoyens et des administrés dans les institutions et services publics, en particulier dans le contexte de la digitalisation de l'administration publique.

Il est primordial que les agents de la fonction publique soient sensibilisés à la sécurité de l'information et des données à caractère personnel. Ils doivent être conscients des risques qui peuvent résulter de comportements inappropriés dans la gestion des informations et données à caractère personnel.

En effet, **un agent bien sensibilisé en la matière contribue à la relation de confiance** qui doit impérativement subsister entre les citoyens et l'administration.

LA SÉCURITÉ DE L'INFORMATION, UNE PRIORITÉ DU GOUVERNEMENT LUXEMBOURGEOIS

La sécurité de l'information et des données à caractère personnel constitue une priorité pour le gouvernement luxembourgeois.

Monsieur le Premier ministre a, dans le cadre de son discours sur l'état de la Nation du 11 octobre 2022, fait l'annonce suivante à la tribune de la Chambre des députés :

> *D'Zuel vun de Cyberattacke geet weltwäit kontinuéierlech erop. Virun allem kritesch Infrastrukturen aus ville Secteuren, mä speziell am Energie- an Telekommunikatiounsberäich sinn an de leschte Joren Zil vu Cyberattacke ginn.*
>
> *Lëtzebuerg ass hei keng Insel. Eng rezent Attack op e grousse lëtzebuergeschen Energiebetrib huet eis dat nach eng Kéier virun Ae gefouert. Dofir setze mir eis national Strategie an der Cybersécherheet konsequent ëm a mir hunn eis Efforten an dësem Beräich nach eng Kéier däitlech verstäerkt.*
>
> *[…]*
>
> *E Liewen ouni Internet ass fir vill Mënschen net méi virstellbar. D'Welt ass haut esou vernetzt, datt och nëmmen eng eenzeg gezielten Attack eisen Alldag, wéi mir e gewinnt sinn, massiv stéiere kéint.*
>
> *Déi fir d'Cybersécherheet zoustänneg Verwaltungen an Autoritéite kréien am nächste Budget an och déi Joren drop däitlech méi Ressourcë fir eist Land beschtméiglechst géint Attacken ze schützen. De Staat, d'Wirtschaft, d'Recherche an d'Bierger mussen hei enk zesumme schaffen.*

La transformation digitale, le déploiement croissant de nouvelles technologies dans les domaines économiques et sociétaux ainsi que la dématérialisation des services fournis aux citoyens nécessitent un renforcement de la sécurité de l'information et des données à caractère personnel.

Des facteurs tels que l'interconnexion entre les systèmes d'information, la multiplication des informations numériques et le nombre croissant des cyberattaques amplifient les risques en termes de sécurité de l'information et de divulgations illicites de données à caractère personnel.

De ce fait, il est indispensable que les administrations étatiques et communales soient en mesure d'éviter qu'un incident de sécurité se produise. Il est également primordial que les réseaux et les systèmes d'information puissent résister de manière appropriée à des actions qui compromettent la disponibilité, l'intégrité ou la confidentialité des informations et des données à caractère personnel traitées.

A noter que la présente publication ne couvre pas les aspects de la sécurité des informations classifiées visées par la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité.

LES ENJEUX DE LA SÉCURITÉ DE L'INFORMATION ET DES DONNÉES À CARACTÈRE PERSONNEL POUR LES ENTITÉS PUBLIQUES

Les enjeux de la sécurité de l'information et des données à caractère personnel sont multiples. Ils comprennent notamment :

La protection des infrastructures critiques nationales

Les infrastructures critiques nationales sont indispensables au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social du pays. Les dépendances intersectorielles des infrastructures critiques sur le plan national, tout comme les dépendances sectorielles sur le plan international, sont très prononcées.

Exemples d'infrastructures critiques :

- **INFRASTRUCTURES D'ÉNERGIE (GAZ, ÉLECTRICITÉ, ETC.)**
- **INFRASTRUCTURES DE DISTRIBUTION D'EAU**
- **RÉSEAUX DE COMMUNICATIONS ÉLECTRONIQUES**
- **INFRASTRUCTURES NUMÉRIQUES**

La protection des infrastructures critiques vise à prévenir, atténuer ou neutraliser le risque d'une réduction de la disponibilité ou d'une discontinuité de ces services d'importance vitale, indispensables au bon fonctionnement de la vie socio-économique.

A cette fin, le Haut-Commissariat à la protection nationale a élaboré des stratégies et des politiques nationales visant la protection des infrastructures critiques ainsi que la reprise d'activité en cas d'incident.

La sécurité des installations publiques et la continuité du service public

La sécurité de l'information est un élément-clé permettant de garantir la sécurité des installations publiques et la continuité du service public.

Elle vise tant la sécurité informatique des réseaux de l'Etat (qui englobe notamment les établissements publics) et des communes que la sécurité physique des infrastructures publiques.

Elle comprend la capacité de prévenir des attaques potentielles, l'aptitude à réduire au minimum les répercussions sur les services en cas d'incident de sécurité ainsi que la faculté de les surmonter rapidement.

Le principe de continuité du service public repose sur la nécessité d'assurer de manière régulière et sans interruption une activité qui réponde à un besoin d'intérêt général menée sous le contrôle de l'administration dans ses prérogatives de puissance publique.

Exemples d'enjeux de la sécurité de l'information :

LA PERTURBATION DES FEUX DE SIGNALISATION PEUT CONDUIRE À UNE DÉSORGANISATION DE LA CIRCULATION ET À DES ACCIDENTS DE LA ROUTE

UNE PANNE INFORMATIQUE PEUT ENTRAÎNER DES DIFFICULTÉS DANS LA COLLECTE DES ORDURES MÉNAGÈRES

LE NON-REMBOURSEMENT OU L'ABSENCE DE VERSEMENT DE PRESTATIONS SOCIALES À DES PERSONNES CONCERNÉES PEUT PLACER CES DERNIÈRES EN SITUATION PRÉCAIRE

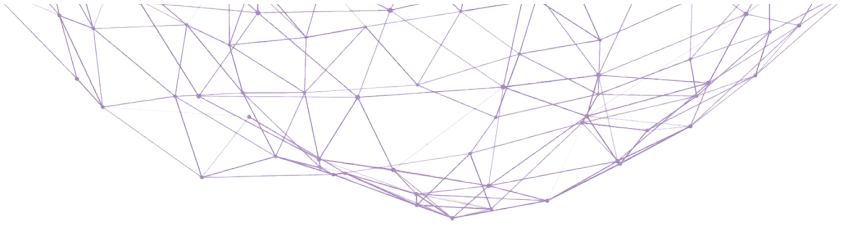
L'IMPOSSIBILITÉ D'ACCÉDER AUX DOSSIERS PATIENTS TENUS ÉLECTRONIQUEMENT PAR UN HÔPITAL EN CAS D'ATTAQUE PAR RANÇONGICIEL PEUT AVOIR DES CONSÉQUENCES NÉGATIVES POUR CERTAINS PATIENTS

Le maintien de la confiance des citoyens à l'égard des administrations

La sécurité de l'information – tout comme le respect des règles de protection des données à caractère personnel – est indispensable afin de maintenir la confiance des citoyens et administrés dans les institutions démocratiques et les services publics.

De ce fait, les administrations étatiques et communales doivent se montrer exemplaires, de surcroît dans un contexte de transformation digitale qui constitue un axe prioritaire de modernisation de l'administration publique.

CHAPITRE 1 //
LES ENTITÉS ÉTATIQUES COMPÉTENTES EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION ET DES DONNÉES À CARACTÈRE PERSONNEL



Garantir la sécurité de l'information et des données à caractère personnel est une tâche complexe. Les administrations étatiques et communales œuvrent dans un environnement exposé, en constante mutation et sous le regard attentif de la presse et des citoyens.

Différents acteurs publics sont impliqués dans ce domaine et jouent un rôle essentiel dans l'analyse des risques potentiels ainsi que dans la prévention et la gestion des incidents de sécurité :

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Haut-Commissariat
à la protection nationale

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

CERT gouvernemental

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

Agence nationale de la sécurité
des systèmes d'information

ctie
Centre des technologies
de l'information de l'État

LHC
Luxembourg House
of Cybersecurity

ILR
INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

CNPD
COMMISSION
NATIONALE
POUR LA
PROTECTION
DES DONNÉES

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Commissariat du gouvernement
à la protection des données
auprès de l'État

SECTION 1 :
LE HAUT-COMMISSARIAT À LA PROTECTION NATIONALE

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Haut-Commissariat
à la protection nationale

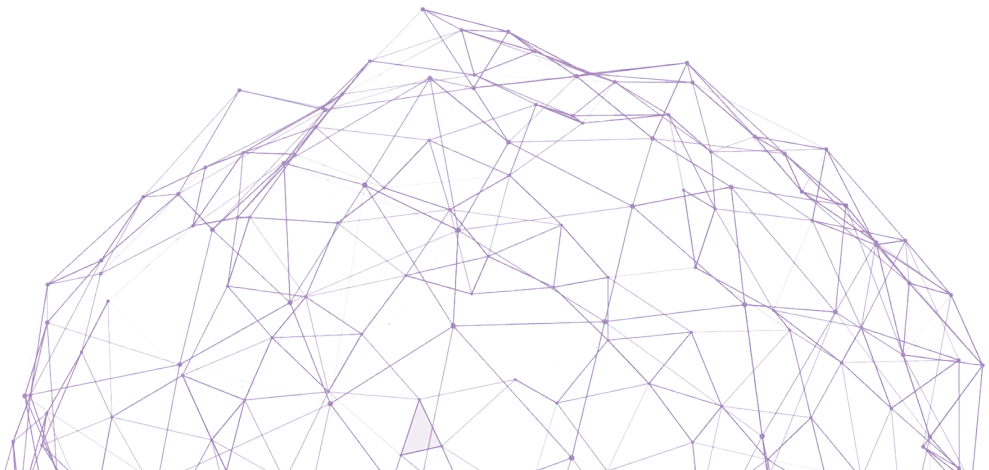
*Le **Haut-Commissariat à la protection nationale** (« HCPN ») est institué par la loi du 23 juillet 2016 portant création du Haut-Commissariat à la protection nationale. Il est placé sous l'autorité du Premier ministre, ministre d'Etat.*

Missions : Prévention et gestion de crises produisant des conséquences graves pour le pays, une partie du pays ou la population.

Le HCPN a notamment pour mission d'assurer la « protection nationale » c'est-à-dire de prévenir tout évènement qui porte préjudice aux intérêts vitaux ou aux besoins essentiels du pays, de coordonner la mise en œuvre des mesures permettant de faire face à une telle crise et de permettre le retour à l'état normal.

Il est ainsi chargé d'assurer la protection des infrastructures critiques, de prévenir et anticiper la survenance de crises et la gestion de crises. A cette fin, il a également pour attribution de coordonner les contributions des différents services de l'Etat, de procéder à l'analyse des risques et à l'organisation d'une veille, ainsi que de développer et de coordonner une stratégie nationale de gestion de crises.

Le HCPN doit initier, conduire et coordonner les tâches de gestion de crises. Il doit veiller à l'exécution de toutes les décisions prises. En matière de cybersécurité, il a notamment adopté un plan de gestion de crise pour faire face aux failles techniques et attaques cybernétiques d'envergure contre les systèmes d'information du secteur public et/ou du secteur privé, de nature à engendrer des conséquences graves pour une partie du territoire ou de la population (Plan d'intervention d'urgence « Cyber »).



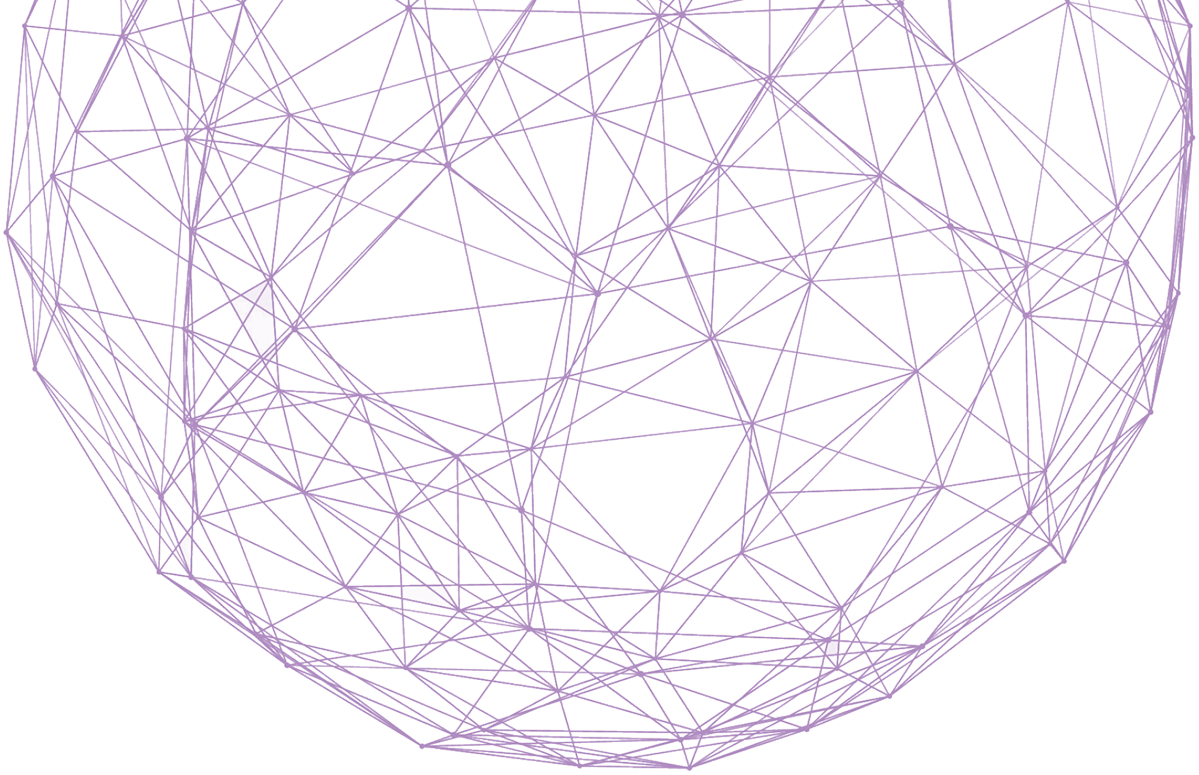
SECTION 2 :
L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale
Agence nationale de la sécurité
des systèmes d'information

*Suivant la loi modifiée du 23 juillet 2016 portant création du Haut-Commissariat à la protection nationale, ce dernier dans sa fonction d'**Agence nationale de la sécurité des systèmes d'Information** (« ANSSI ») contribue à la mise en œuvre de la politique générale de sécurité de l'information de l'Etat et de lignes directrices en cette matière, définit une approche de gestion des risques et contribue à la sensibilisation et la formation des agents de l'Etat en matière de sécurité de l'information.*

Missions : L'ANSSI a la charge :

- de contribuer à la mise en œuvre de la politique générale de sécurité de l'information de l'Etat ;
- de contribuer à la mise en œuvre, en concertation avec les administrations et services de l'Etat, des politiques et lignes directrices de sécurité de l'information portant sur les domaines de la politique générale de sécurité de l'information de l'Etat et des nouvelles technologies de l'information et de la communication ;
- d'émettre des recommandations d'implémentation des politiques et lignes directrices de sécurité de l'information et d'assister les administrations et services de l'Etat au niveau de l'implémentation des mesures proposées ;
- de définir, en concertation avec les administrations et services de l'Etat, une approche de gestion des risques, en vue de constituer un plan d'évaluation et d'identification des risques concernant la sécurité de l'information et d'accompagner, à leur demande, les administrations et services de l'Etat dans l'analyse et la gestion des risques ;



- de conseiller l'Institut national d'administration publique, respectivement, à leur demande, les administrations et services de l'Etat dans la définition d'un programme de formation dans le domaine de la sécurité de l'information ;

- de promouvoir la sécurité de l'information par le biais de mesures de sensibilisation ;

- de conseiller, à leur demande, les établissements publics et les infrastructures critiques en matière de sécurité des réseaux et systèmes d'information et des risques y liés ;

- d'assurer la fonction d'autorité TEMPEST en veillant à la conformité des réseaux et systèmes d'information classifiés aux stratégies et lignes directrices TEMPEST et en approuvant les contre-mesures TEMPEST pour les installations et les produits destinés à protéger des pièces classifiées jusqu'à un certain niveau de classification dans leur environnement opérationnel.

SECTION 3 :
LE CENTRE DE TRAITEMENT DES URGENCES INFORMATIQUES

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

CERT gouvernemental

Suivant la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la protection nationale, ce dernier dans sa fonction de ***CERT Gouvernemental*** *(« GOVCERT ») constitue le point de contact unique dédié au traitement des incidents de sécurité d'envergure affectant les réseaux et les systèmes d'informations des administrations et services de l'Etat, assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques et aux incidents de sécurité d'envergure et assure les fonctions de centre national de traitement des urgences informatiques (CERT National) et de centre militaire de traitement des urgences informatiques (CERT Militaire).*

Missions : Le GOVCERT a pour missions :

- de constituer le point de contact unique dédié au traitement des incidents de sécurité d'envergure affectant les réseaux et les systèmes d'information des administrations et services de l'Etat et, à leur demande, des établissements publics et des infrastructures critiques ;
- d'assurer un service de veille, de détection, d'alerte et de réaction aux attaques informatiques et aux incidents de sécurité d'envergure affectant les réseaux et systèmes d'information des administrations et services de l'Etat et, à leur demande, des établissements publics et des infrastructures critiques ;
- d'assurer la fonction de centre national de traitement des urgences informatiques, dénommé CERT National, en :
    - opérant comme le point de contact officiel national pour les CERTs nationaux et gouvernements étrangers ;
    - opérant comme le point de contact officiel national pour la collecte et la distribution d'informations relatives aux incidents de sécurité qui concernent les réseaux et systèmes d'information implantés au Luxembourg ;
    - relayant les informations collectées aux CERTs sectoriels en charge de la cible d'une attaque ou à défaut de CERT sectoriel, directement à la cible ;

- d'assurer la fonction de centre militaire de traitement des urgences informatiques, dénommé CERT Militaire, en :
    - opérant comme le point de contact officiel national pour les CERTs militaires étrangers ;
    - assurant un service de veille, de détection, d'alerte et de réaction aux attaques informatiques et aux incidents de sécurité d'envergure affectant les réseaux et les systèmes d'information de l'armée à partir du territoire du Grand-Duché ;
    - opérant, à partir du territoire du Grand-Duché, une équipe d'intervention spécialisée capable de prendre en charge la réponse aux incidents de sécurité d'envergure liés à ces réseaux et systèmes d'information.

Le GOVCERT assure la fonction de Centre national de traitement des urgences informatiques (CERT national). Ainsi, il constitue le point de contact officiel national pour la collecte et la distribution d'informations relatives aux incidents de sécurité qui concernent les systèmes d'information et de communication implantés au Luxembourg.

Dans le cadre de ses missions, le GOVCERT est par ailleurs autorisé à demander des informations à caractère technique sur les infrastructures de communication et d'information, sur les fichiers de journalisation techniques hors informations contenant des données à caractère personnel (sauf pour les fichiers de journalisation ayant comme finalité la protection des biens de l'Etat) et à exiger des administrations et services de déconnecter des équipements informatiques des réseaux de communication de l'Etat.

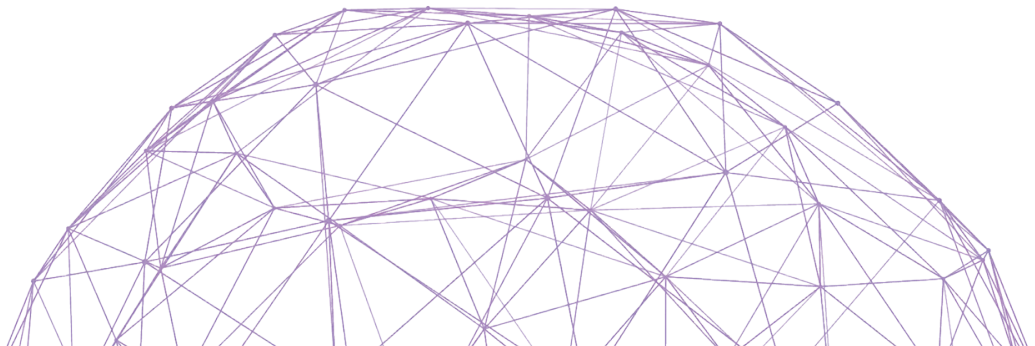
SECTION 4 :
LE COMITÉ INTERMINISTÉRIEL DE COORDINATION EN MATIÈRE DE CYBERPRÉVENTION ET DE CYBERSÉCURITÉ

*Le **Comité interministériel de coordination en matière de cyberprévention et de cybersécurité** est constitué du HCPN, du HCPN-ANSSI, du HCPN-GOVCERT, du Ministère de l'Economie, du Département de la défense, du Ministère d'Etat - Service des médias, de la connectivité et de la politique numérique, du Service de Renseignement de l'Etat, de la Luxembourg House of Cybersecurity, du Centre des technologies de l'information de l'Etat, du Ministère des Affaires étrangères et européennes et de l'Institut luxembourgeois de régulation. Il est institué sur base d'une décision du Conseil de gouvernement du 6 décembre 2017.*

Missions : Coordination et cohérence des initiatives et des mesures adoptées en matière de cyberprévention et de cybersécurité.

Le Comité interministériel de coordination en matière de cyberprévention et de cybersécurité a pour mission de veiller à la coordination et à la cohérence des initiatives et mesures adoptées en matière de sécurité de l'information et de contrôler la mise en œuvre au niveau national des politiques de cybersécurité adoptées.

Par ailleurs, il est chargé de conseiller le gouvernement en matière de cyberprévention et de cybersécurité en identifiant les sujets et priorités à approfondir dans ce domaine.



SECTION 5 :
LE CENTRE DES TECHNOLOGIES DE L'INFORMATION DE L'ETAT

ctie
Centre des technologies de l'information de l'État

*Le **Centre des technologies de l'information de l'Etat** (« CTIE ») est institué par la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat. Il est placé sous l'autorité du ministre ayant les Technologies de l'information de l'Etat dans ses attributions.*

Missions : Gestion de la sécurité de l'informatique et administration du réseau informatique commun de l'Etat.

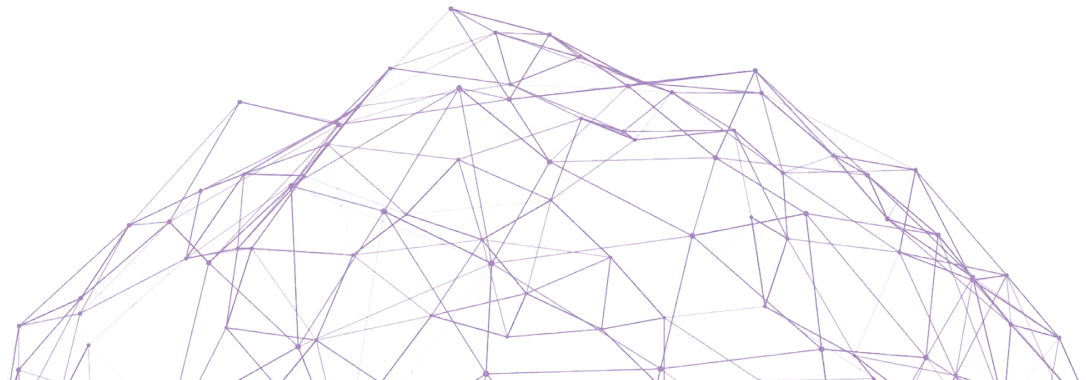
Le CTIE est en charge des services IT pour le gouvernement, les ministères et les administrations luxembourgeoises. Il est responsable de la mise en œuvre de la sécurité des infrastructures IT de l'Etat dont notamment le réseau de communication sécurisé de l'Etat.

Outre la sécurité informatique, les services du CTIE couvrent tous les domaines de l'IT incluant :

- l'infrastructure réseau et de communication,
- le « hosting »,
- le « cloud » privé (IaaS),
- les plateformes (PaaS),
- les solutions logicielles génériques et sur mesure (SaaS),
- les services annexes tels que la génération de documents sécurisés, l'impression en masse individualisée, etc.

Il gère également la bureautique et la téléphonie des ministères et administrations.

Le CTIE, acteur central en matière d'eGovernment, met en œuvre le portail en ligne « Guichet.lu », le « single point of contact » pour les citoyens et entreprises pour la réalisation de leurs démarches avec l'Etat, ainsi que la plateforme interactive « MyGuichet.lu ».



SECTION 6 : LA LUXEMBOURG HOUSE OF CYBERSECURITY

*La **Luxembourg House of Cybersecurity** (« LHC »), groupement d'intérêt économique, est l'agence nationale de cybersécurité au service de l'économie luxembourgeoise et des communes.*

Missions : Soutien aux entreprises, communes et citoyens du Luxembourg afin d'accroître la résilience de l'économie nationale face aux menaces « cyber ».

La LHC oriente son travail sur la valorisation et le développement de l'innovation, des compétences, de la collaboration et du renforcement des capacités dans le domaine de la cybersécurité.

L'agence est composée de deux centres d'expertise :

- le « Computer Incident Response Center Luxembourg » (« CIRCL ») est une initiative gouvernementale conçue pour fournir une réponse systématique aux menaces et incidents de sécurité informatique.

  Le CIRCL est le CERT (Computer Emergency Response Team) pour le secteur privé, les communes et les entités non gouvernementales au Luxembourg.

  Le CIRCL fournit une large gamme de services à différentes échelles :

  - coordination et traitement des incidents,
  - outils et services d'aide au traitement des incidents,
  - flux de données et réseau de détection précoce,
  - partage d'informations.

- le « National Cybersecurity Competence Centre » (NC3), qui a pour mission de soutenir le développement de capacités et de compétences en cybersécurité et de contribuer à la recherche et au développement technologique en la matière. Il constitue une plateforme d'échange et d'expertise au niveau communal pour toute question touchant à la sécurité de l'information des communes.

  La mission du NC3 repose sur les 3 piliers suivants :

  - encourager et coordonner le renforcement des capacités et compétences en matière de cybersécurité pour les organisations ou personnes exposées ainsi que pour les prestataires de services de sécurité ;
  - développer une base industrielle solide en matière de cybersécurité au Luxembourg et dans la Grande Région afin de soutenir un écosystème de plus en plus numérisé ;
  - orienter les efforts de recherche et l'excellence technologique en matière de cybersécurité sur base d'une analyse avancée du volume croissant de données pertinentes.

SECTION 7 : L'INSTITUT LUXEMBOURGEOIS DE RÉGULATION

ILR

INSTITUT LUXEMBOURGEOIS DE RÉGULATION

*L'**Institut luxembourgeois de régulation** (« ILR ») est un établissement public institué par la loi modifiée du 30 mai 2005 portant organisation de l'Institut luxembourgeois de régulation.*

Missions : Surveillance de la mise en place de mesures de sécurité nécessaires par les opérateurs de services essentiels qui relèvent de sa compétence et les fournisseurs de réseaux et de services de communications électroniques et gestion des notifications d'incidents de ces derniers.

L'ILR a pour mission de contribuer à préserver la sécurité des réseaux et services de communications électroniques.

Dans le cadre des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne, il a pour mission de s'assurer spécifiquement que les opérateurs de services essentiels des secteurs qui relèvent de sa compétence prennent les mesures nécessaires pour prévenir les incidents et gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent dans le cadre de leurs activités. Cela concerne les secteurs de l'énergie, du transport, de la santé, de l'eau potable et des infrastructures numériques ainsi que les fournisseurs de services numériques.

Par ailleurs, l'ILR constitue le point de contact national unique en matière de sécurité des réseaux et des systèmes d'information. Il reçoit également les notifications des opérateurs de services essentiels concernant l'analyse de risques, les mesures de sécurité en place ainsi que les incidents. A noter que pour le secteur financier, ce rôle est assuré par la Commission de surveillance du secteur financier (CSSF).

SECTION 8 :
LE COMMISSARIAT DU GOUVERNEMENT À LA PROTECTION DES DONNÉES AUPRÈS DE L'ETAT

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Commissariat du gouvernement
à la protection des données
auprès de l'État

*Le **Commissariat du gouvernement à la protection des données auprès de l'Etat** (« CGPD ») est une administration instituée par la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.*

Missions : Contribution au développement de la protection des données à caractère personnel au sein de l'administration étatique et conseils dans la mise en place de mesures appropriées pour protéger les droits et libertés des personnes concernées.

Le CGPD a pour mission générale de contribuer au développement de la protection des données à caractère personnel au sein de l'administration étatique.

Il contribue également à une mise en œuvre cohérente des politiques dans le domaine de la protection des données à caractère personnel au sein de l'Etat. A cette fin, il conseille, sur demande, les membres du gouvernement et accompagne les chefs d'administration dans la mise en place de mesures appropriées pour protéger les droits et libertés des personnes concernées.

Par ailleurs, le CGPD peut être désigné comme délégué à la protection des données par les ministres ou leurs chefs d'administration, ainsi que par les communes. En outre, il assiste les délégués à la protection des données que les administrations étatiques ont désignés en interne.

Dans le cadre de ses missions de promotion des bonnes pratiques en matière de protection des données au sein de l'administration étatique, le CGPD sensibilise les agents publics afin de leur permettre d'acquérir les bons réflexes en la matière dans l'exécution de leurs tâches quotidiennes au sein de leur administration. Pour ce faire, des séances d'initiation à la protection des données et des formations spécialisées dédiées aux différents aspects du règlement (UE) 2016/679 du 27 avril 2016 (règlement général sur la protection des données ; ci-après « RGPD ») sont régulièrement offertes aux agents de l'Etat et des communes. Le CGPD développe par ailleurs des documents et des outils adaptés visant à assister les entités en matière de conformité au RGPD.

SECTION 9 : LA COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

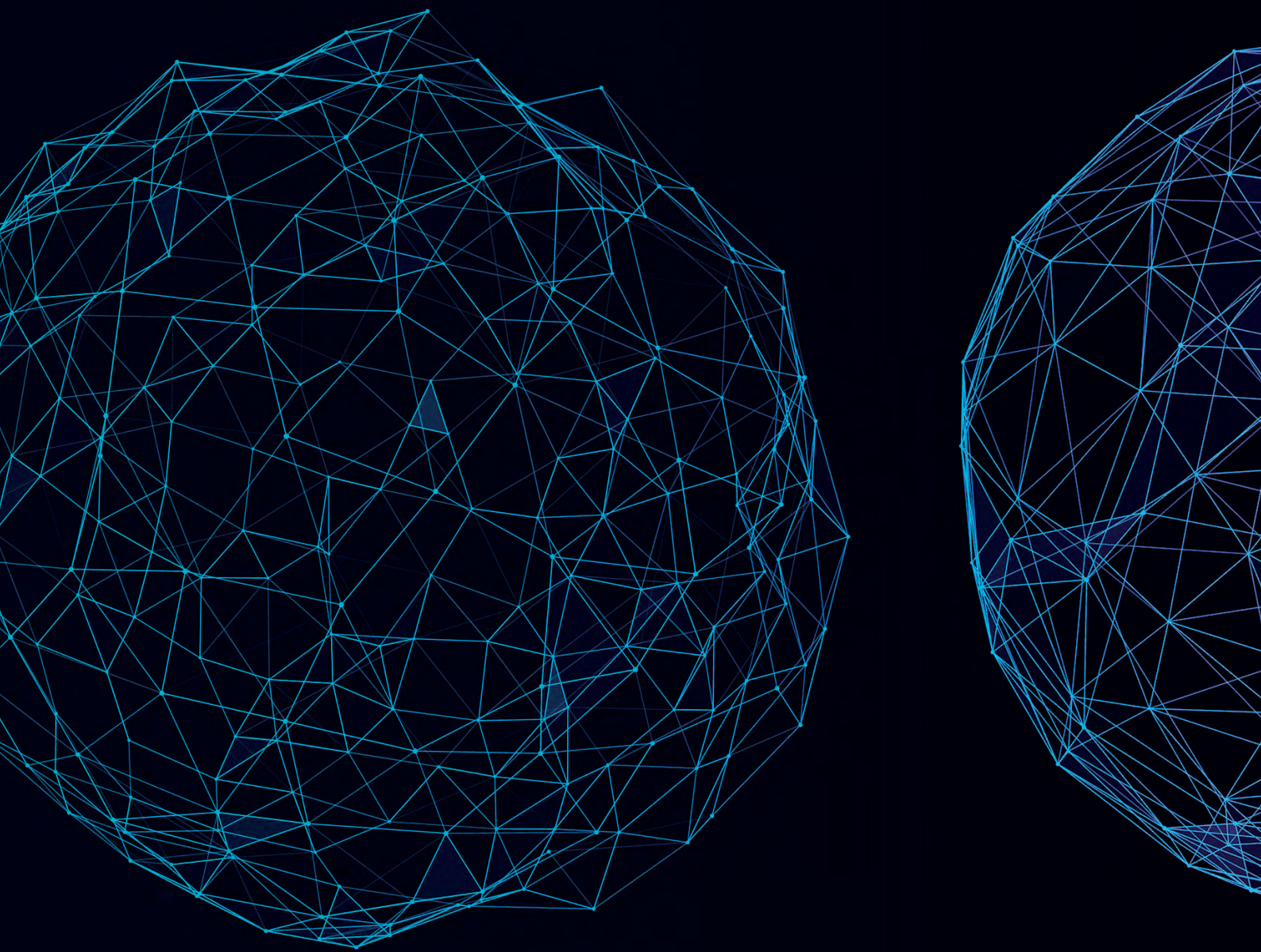
*La **Commission nationale pour la protection des données** (« CNPD ») est l'autorité de contrôle de la protection des données au Luxembourg. Créée en 2002, il s'agit d'un établissement public disposant d'une autonomie financière et administrative et doté de la personnalité juridique.*

Missions : Conseil, sensibilisation et contrôle des responsables du traitement de données à caractère personnel sur le respect des exigences du RGPD dont l'obligation de sécurité des données.

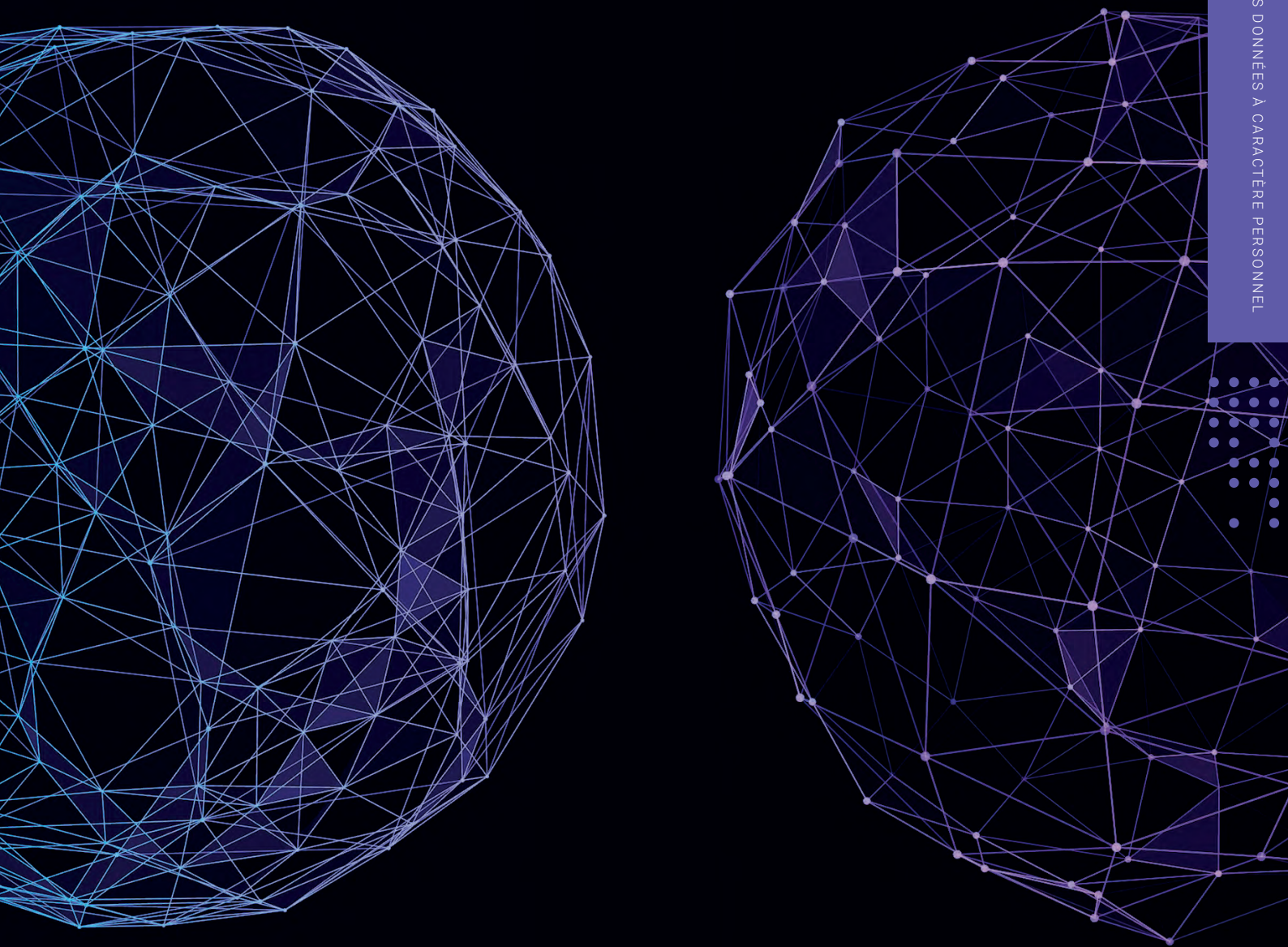
Depuis la loi du 1er août 2018 portant organisation de la CNPD et du régime général sur la protection des données, la CNPD se charge de deux grandes missions, à savoir : d'une part le volet « conseil » et d'autre part le volet « contrôle » :

- Le volet « conseil » regroupe les activités de guidance et de sensibilisation à travers l'organisation de formations et de conférences s'adressant au grand public, ainsi qu'aux experts en matière de protection des données. La CNPD est également sollicitée pour répondre aux demandes des personnes concernées sur l'exercice de leurs droits, publier des guidances thématiques, rédiger des avis juridiques et aviser des projets de loi ou de mesures réglementaires du gouvernement ;
- Le volet « contrôle » comprend le traitement des réclamations introduites par une personne concernée ou par une organisation, le traitement des notifications de violations de données personnelles déclarées à la CNPD, ainsi que les enquêtes que la CNPD décide de mener auprès des responsables du traitement et de leurs sous-traitants.

Avec l'entrée en application du RGPD, la CNPD a également un pouvoir de sanction et peut donc prononcer des mesures correctrices, des suspensions de traitements de données personnelles et des amendes administratives. Dans le cadre de réclamations transfrontalières, la CNPD coopère avec les autres autorités de contrôle européennes. Elle représente le Luxembourg au sein du Comité européen de la protection des données (European Data Protection Board - « EDPB »). Cet organe européen contribue à garantir que la législation en matière de protection des données est appliquée de façon systématique et cohérente au sein de l'Union Européenne. Il assure également une coopération efficace entre les autorités de contrôle.



CHAPITRE 2 //
L'OBLIGATION DE GARANTIR LA SÉCURITÉ DE L'INFORMATION ET DES DONNÉES À CARACTÈRE PERSONNEL



SECTION 1 :
LES CONCEPTS DE SÉCURITÉ DE L'INFORMATION ET DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

LA DIFFÉRENCE ENTRE « INFORMATION » ET « DONNÉE À CARACTÈRE PERSONNEL »

La notion d'**« information »** est plus large que celle de **« donnée à caractère personnel »** définie par le RGPD (ci-après aussi « données »).

Contrairement à la « donnée à caractère personnel », l'« information » ne vise pas seulement les renseignements se rapportant à un individu. Elle englobe de manière plus large toute information indépendamment de son type, de son contenu ou de son support.

Dès lors qu'une « information » se rapporte à une personne physique identifiée ou identifiable, elle constitue une « donnée à caractère personnel » au sens du RGPD.

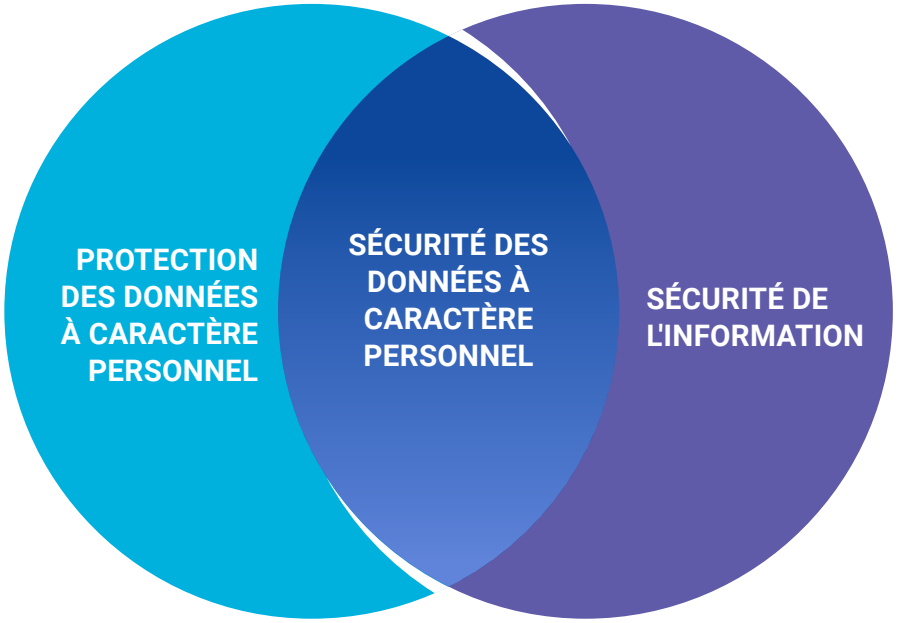
Qu'est-ce qu'une personne physique identifiée ou identifiable au sens du RGPD ?

Le RGPD dispose qu'une personne physique est réputée être « identifiable » lorsqu'elle peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, le numéro de matricule ou un autre numéro d'identification, des données de localisation, un identifiant en ligne, ou encore moyennant un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

LA SUPERPOSITION DES CONCEPTS DE « SÉCURITÉ DE L'INFORMATION » ET DE « PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL »

La « sécurité de l'information » et la « protection des données » au sens du RGPD sont deux concepts différents qui, toutefois, se recoupent.

Ainsi, l'on peut parler d'une **superposition des concepts** qui ont en commun le domaine de la **sécurité des données à caractère personnel au sens du RGPD.**



La sécurité de l'information

La sécurité de l'information vise toutes les informations qui méritent d'être protégées en raison de leur valeur pour l'entité qui les détient et des risques qu'une atteinte, en particulier, à la confidentialité, l'intégrité, la disponibilité ou la traçabilité de ces informations pourrait avoir.

Contrairement à la protection des données, qui est axée sur les droits et libertés des individus, la sécurité de l'information concerne tous les intérêts de l'administration qui méritent d'être protégés (ex. : protection du secret professionnel, protection du secret d'affaires, protection des infrastructures critiques nationales).

Les risques « classiques » à prendre en compte par toute organisation dans le domaine de la sécurité de l'information sont multiples et comprennent, notamment :

LES RISQUES FINANCIERS

LES RISQUES DE RÉPUTATION

LES RISQUES OPÉRATIONNELS

LES RISQUES JURIDIQUES

Les incidents de sécurité peuvent gravement porter atteinte aux intérêts de l'administration en ayant un impact, notamment sur sa réputation, ses intérêts économiques et, voire même, à la sécurité de l'Etat (ex. : la perte ou le vol de documents confidentiels).

La protection des données à caractère personnel

Les droits fondamentaux à la vie privée et à la protection des données visent à protéger des valeurs fondamentales, telles que l'autonomie et la dignité humaine, en accordant une sphère privée aux individus leur permettant de se développer et de s'épanouir librement.

Ces droits constituent des prérequis nécessaires pour l'exercice des autres libertés fondamentales dont jouissent les individus dans une société démocratique, en particulier la liberté d'expression et la liberté de réunion et d'association.

Dans cette perspective, le RGPD requiert que les données à caractère personnel soient traitées de façon à garantir un niveau de sécurité adapté aux risques à l'aide de mesures techniques et organisationnelles appropriées.

Qu'est-ce qu'un « traitement de données » au sens du RGPD ?

Le RGPD définit le « traitement de données » comme « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel ».

Sont notamment concernées les opérations suivantes :

- *la collecte,*
- *la consultation,*
- *l'utilisation,*
- *l'enregistrement,*
- *la structuration,*
- *la conservation (l'hébergement, y compris les « backup »),*
- *la transmission,*
- *la modification,*
- *l'effacement.*

Pour ce faire, le responsable du traitement ne doit pas seulement tenir compte des enjeux classiques de la sécurité de l'information. Il doit également prendre en considération des éléments comme :

- la nature, la portée, le contexte et les finalités du traitement de données, ainsi que
- les « risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques ».

La sécurité des données à caractère personnel s'applique quel que soit le support de l'information et quelle que soit la nature de l'information. Ainsi, les données peuvent être contenues sur un(e) :

NOTE SUR UN POST-IT | **DOCUMENT PAPIER** | **FICHIER INFORMATIQUE** | **PHOTO** | **VIDÉO** | **ENREGISTREMENT AUDIO**

SECTION 2 :
L'OBLIGATION DE GARANTIR LA SÉCURITÉ DES DONNÉES CONFORMÉMENT AU RGPD

L'administration doit traiter les données de façon à en garantir une sécurité appropriée, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques et organisationnelles appropriées.

La sécurité des données est un volet essentiel du RGPD. Les données doivent être traitées de manière à ce que leur sécurité puisse être garantie et de manière à éviter, en particulier :

- le traitement illicite de données,
- la divulgation non autorisée ou illicite de données,
- la perte (temporaire ou définitive) de données,
- la destruction illicite de données,
- les défaillances (techniques ou organisationnelles) des systèmes d'information.

L'OBLIGATION DE GARANTIR UN NIVEAU DE SÉCURITÉ ADÉQUAT

L'administration en charge du traitement de données (le « responsable du traitement » au sens du RGPD) doit mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adéquat.

Exemples de différents types de mesures appropriées :

LA MISE EN PLACE D'UN SYSTÈME DE SAUVEGARDE (« BACKUP »)

LA PSEUDONYMISATION OU L'ANONYMISATION DE DONNÉES

LA SENSIBILISATION DU PERSONNEL

LES ENCADREMENTS CONTRACTUELS

LA TRAÇABILITÉ DES ACCÈS ET DES ACTIONS

LE CHIFFREMENT DES DONNÉES

LA SÉGRÉGATION DES ACCÈS AU REGARD DES FONCTIONS ET DES TÂCHES DES AGENTS

LES PROCÉDURES ET POLITIQUES INTERNES

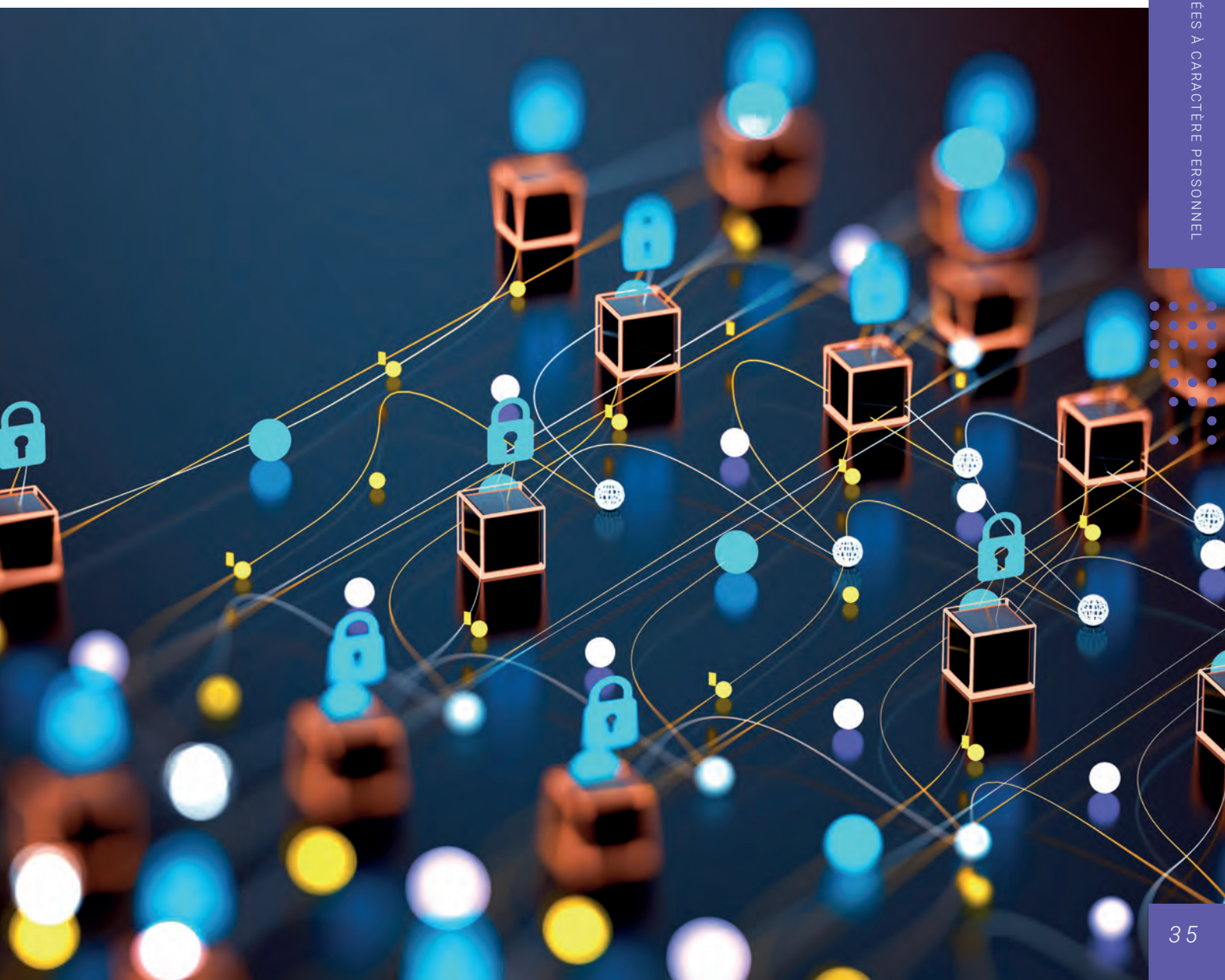
L'objectif de ces mesures est de garantir, en particulier :

- **la confidentialité des données** : les données doivent être traitées de manière à n'être accessibles qu'aux administrations et agents pour accomplir leurs missions dans le respect du principe du besoin d'en connaitre (« need to know ») ;

- **l'intégrité des données** : les données doivent être traitées de telle manière que leur exactitude et authenticité soient garanties. En d'autres termes, les données doivent être fiables, complètes et ne pas être modifiées de manière non autorisée ou accidentelle ;

- **la disponibilité des données** : les données doivent, à tout moment, être disponibles à l'administration dans l'accomplissement de ses missions ;

- **la résilience constante des systèmes et des services de traitement** : l'administration doit pouvoir assurer la continuité des systèmes d'information et de traitement de données, nonobstant les attaques externes ou les mauvaises manipulations effectuées dans les systèmes.



LA PROTECTION DES DONNÉES DÈS LA CONCEPTION ET PAR DÉFAUT

Dans un objectif de **protection des données dès la conception** (« privacy by design ») et de **protection des données par défaut** (« privacy by default »), l'administration responsable du traitement de données doit :

- adopter des mesures techniques et organisationnelles appropriées pour protéger les droits de la personne concernée, telles que la pseudonymisation, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même ;

- s'assurer que, par défaut, seules les données nécessaires au regard des finalités spécifiques du traitement de données sont traitées (la finalité du traitement étant l'objectif ou l'ensemble d'objectifs en vue duquel le traitement des données est opéré).

Par exemple :

- *Au moment de la conception d'un formulaire de collecte de données auprès du citoyen, l'administration doit, dans la mesure du possible, éviter les champs de texte libre en faveur d'un système de choix prédéterminés concis (cases à cocher). Cette mesure permet de réduire les imprécisions et d'éviter une collecte de données allant au-delà de ce qui est nécessaire au regard des finalités du traitement. Une telle mesure contribue à la confidentialité et à l'intégrité des données. L'administration doit également veiller à ce que seuls les agents dûment habilités puissent accéder aux données dont ils ont besoin pour l'accomplissement de leurs tâches professionnelles, et ceci en fonction de leur rôle. Selon les circonstances et la sensibilité des données, un système d'authentification forte (ex. : « Luxtrust ») devrait être envisagé.*
- *Plutôt que de transmettre à une autre administration le dossier complet d'un administré, le responsable du traitement initial devrait s'assurer que seules les données strictement nécessaires pour l'accomplissement des missions du destinataire, conformément à la législation applicable, fassent l'objet de la transmission (ex. : les valeurs numériques sollicitées ainsi que les coordonnées de la personne concernée). Il va sans dire que le responsable du traitement initial devrait uniquement transmettre les données à une autre administration dans le respect des conditions prévues par le RGPD.*

L'« ACCOUNTABILITY » DU RESPONSABLE DU TRAITEMENT

La charge de garantir une sécurité appropriée des données incombe à l'administration agissant en tant que responsable du traitement.

Qui est le « responsable du traitement » au sens du RGPD ?

Le responsable du traitement est la personne ou l'entité (une personne physique ou morale, une autorité publique, un service ou un autre organisme) qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données.

La charge d'assurer le respect des principes de la protection des données incombe au responsable du traitement (généralement l'entité en tant que telle, et non un individu au sein de l'entité). Ce dernier peut être désigné par la loi. Dans le cas contraire, il convient d'analyser les éléments factuels du cas concret et les circonstances dans lesquelles l'opération de traitement de données est réalisée pour déterminer qui est le responsable du traitement.

Pour ce faire, il convient de tenir compte des deux facteurs suivants :

- *qui détermine **les finalités du traitement, c'est-à-dire le « pourquoi » du traitement** (qui décide quelles données sont collectées et qui définit les objectifs pour lesquels ces données sont traitées ?) ;*
- *qui détermine **les moyens essentiels du traitement, c'est-à-dire le « comment » du traitement** (qui décide par quels instruments les données sont collectées et comment ces dernières sont traitées ?).*

L'administration doit, en collaboration étroite avec ses éventuels sous-traitants, mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

Elle doit également être en mesure de prouver que ces mesures ont été mises en œuvre et qu'elles sont effectives. Ces mesures doivent, en outre, être actualisées, si nécessaire.

Dans une optique d'accountability, l'administration en charge du traitement de données doit documenter la mise en place des mesures pour la sauvegarde des droits et libertés des personnes concernées.

LE RÔLE DU DÉLÉGUÉ À LA PROTECTION DES DONNÉES ET DU RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

S'il est vrai que la responsabilité de mettre en place les mesures techniques et organisationnelles revient à l'administration responsable du traitement de données, le délégué à la protection des données et le responsable de la sécurité des systèmes d'information jouent également un rôle important.

Le délégué à la protection des données (« DPD »)

La désignation du DPD est obligatoire pour toutes les autorités publiques. Elle doit être notifiée par le responsable du traitement à la CNPD.

Le DPD doit avoir les qualités professionnelles requises et exercer ses fonctions en toute indépendance. Il ne peut pas exercer d'autres missions et tâches qui entraîneraient un conflit d'intérêts.

Il peut être un membre du personnel du responsable du traitement (DPD interne) ou exercer ses missions sur la base d'un contrat de service (DPD externe). A noter que lorsque le responsable du traitement est une autorité publique ou un organisme public, un seul DPD peut être désigné pour plusieurs d'entre eux, compte tenu de leur structure organisationnelle et de leur taille.

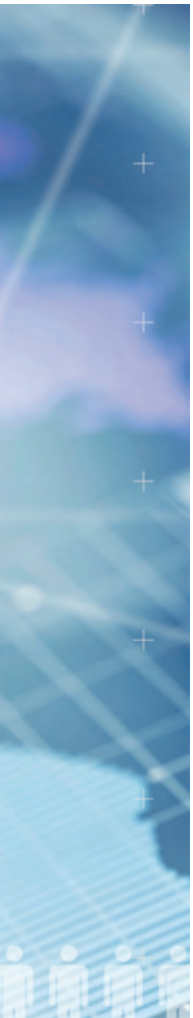
La loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données dispose que les ministres du ressort ou, sous leur autorité, les chefs d'administration compétents **peuvent désigner le CGPD comme leur DPD**. Cette même faculté est offerte aux communes.

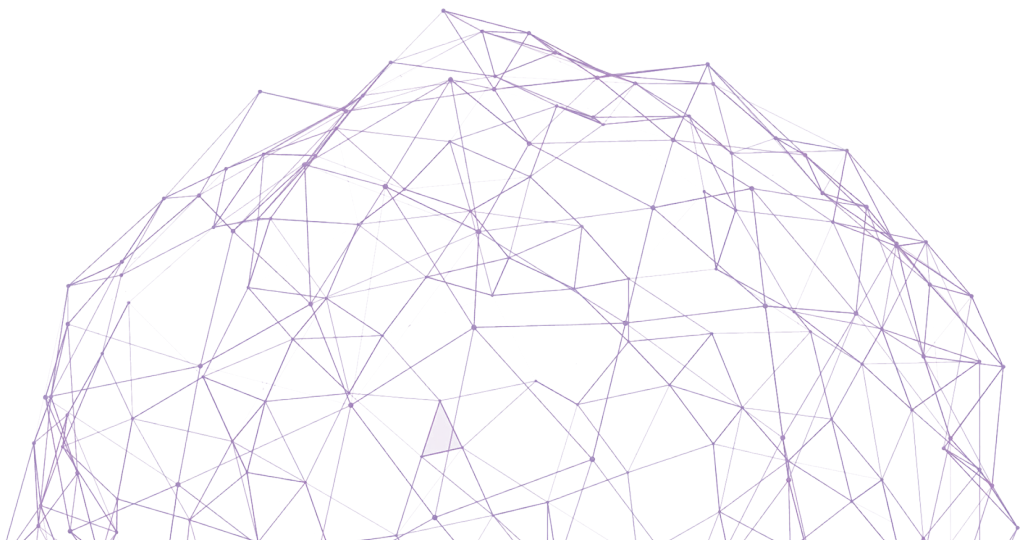
Les missions du DPD sont, en particulier, d'informer et conseiller le responsable du traitement sur les obligations applicables en matière de protection des données, d'en contrôler le respect et de dispenser des conseils, sur demande, en ce qui concerne l'analyse des impacts relatifs aux traitements. Par ailleurs, il doit coopérer avec la CNPD et faire office de point de contact pour cette dernière.

D'après les autorités de protection de données, ***il est essentiel que le DPD, ou son équipe, soit associé au stade le plus précoce possible*** *à toutes les questions inhérentes à la protection des données.*

S'y ajoute que ***le DPD doit disposer du soutien du responsable du traitement*** *(en particulier en termes de ressources et d'accès aux informations liées aux traitements de données) pour pouvoir exercer ses missions conformément au RGPD.*

D'après les autorités de contrôle, l'esprit du RGPD est de faire du DPD le « chef d'orchestre » de la gestion des données au sein de l'entité qui l'a désigné. Pour qu'il puisse assumer ce rôle, le DPD doit être pleinement intégré aux activités opérationnelles du responsable du traitement et agir comme pivot central de la gouvernance des données en lien notamment avec le responsable de la sécurité des systèmes d'information et les services en charge des technologies de l'information.





Le responsable de la sécurité des systèmes d'information (« RSSI »)

Alors que le DPD est chargé de conseiller le responsable du traitement en matière de protection des données, **le RSSI joue un rôle essentiel dans l'identification et la sécurisation des systèmes d'information**, en particulier en élaborant la politique de sécurité de l'information et en s'assurant de son application.

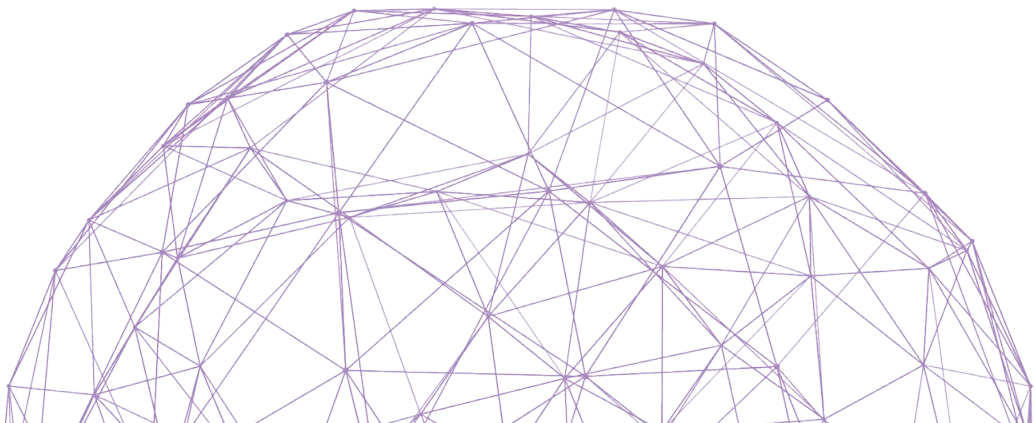
Le RSSI est chargé de veiller à la mise en place de solutions garantissant la sécurité adéquate de l'information et de leurs systèmes de traitement.

Les missions du RSSI sont, notamment :

- *émettre des bonnes pratiques en matière de sécurité de l'information ;*
- *élaborer des politiques spécifiques en la matière et veiller à leur application ;*
- *informer et assister la direction et les services opérationnels afin que la sécurité de l'information soit prise en compte dès la conception et de manière continue ;*
- *gérer la classification et l'accès à l'information ;*
- *assurer la continuité des activités en cas d'incident majeur ou de sinistre ;*
- *sensibiliser le personnel et la direction de son entité en sécurité de l'information ;*
- *promouvoir et coordonner la sécurité de l'information dans son entité ;*
- *collaborer avec le DPD sur les aspects de la protection des données.*

Contrairement à la désignation du DPD qui est obligatoire de par la loi pour les autorités publiques, la désignation du RSSI reste facultative sous le cadre légal actuel. À noter qu'au sein de l'Etat, le RSSI est connu sous la désignation de « Délégué à la Sécurité de l'Information (DSI) ».

La sécurisation des données au sens du RGPD nécessite ainsi une étroite collaboration entre tous les acteurs impliqués dans la sécurité de l'information et dans la protection des données à caractère personnel.



SECTION 3 :
L'ÉVALUATION DES RISQUES ET LA MISE EN ŒUVRE DE MESURES APPROPRIÉES CONFORMÉMENT AU RGPD

Pour déterminer les mesures appropriées à mettre en oeuvre, l'administration responsable du traitement de données doit prendre en compte, entre autres :

- la nature, la portée, le contexte, les finalités du traitement de données, ainsi que
- les « risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques ».

Le RGPD précise qu'un traitement de données peut entraîner des dommages physiques, matériels ou moraux pour la personne concernée tels que :

UNE DISCRIMINATION

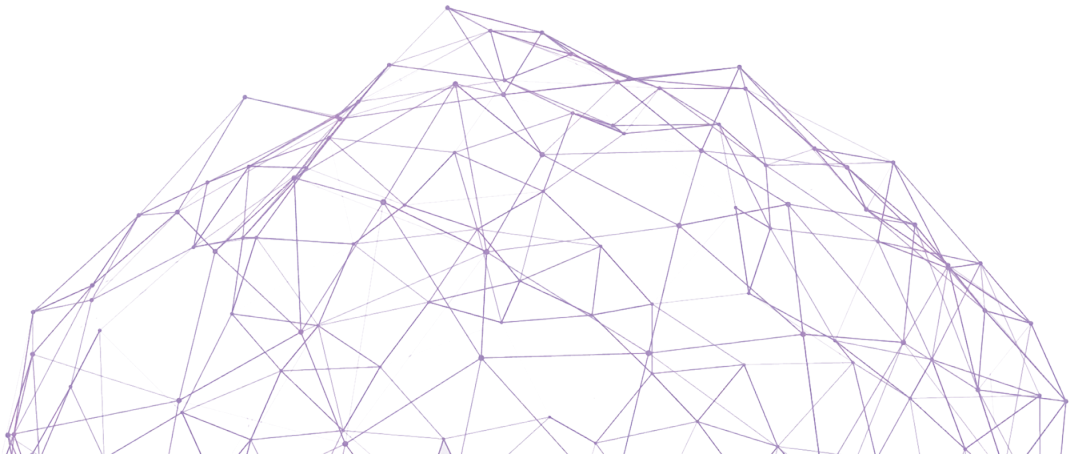
UNE PERTE DE CONFIDENTIALITÉ DE DONNÉES PROTÉGÉES PAR LE SECRET PROFESSIONNEL

UN VOL OU UNE USURPATION D'IDENTITÉ

UNE PERTE FINANCIÈRE

UNE ATTEINTE À LA RÉPUTATION DE LA PERSONNE CONCERNÉE

UN DOMMAGE ÉCONOMIQUE OU SOCIAL IMPORTANT



Tout comme les risques peuvent être de différentes natures, **les mesures appropriées** pour les maîtriser ou les réduire à un niveau acceptable **peuvent prendre différentes formes.**

Par exemple :

Une base de données d'un professionnel de santé qui contient des données médicales ou un fichier des autorités judiciaires contenant des données sur les condamnations pénales des individus nécessite davantage de mesures de sécurité qu'un fichier avec les noms, les prénoms et les données de contact des agents ayant accès à la cantine.

Les mesures appropriées à mettre en place **peuvent être d'ordre technique ou organisationnel et consistent souvent en une combinaison des deux**.

La sécurité des données ne se limite pas à la mise en place d'un ensemble de mesures appliquées aux systèmes d'information. Elle comporte également une dimension « humaine ». Le personnel traitant les données doit adopter un comportement adéquat dans la gestion des données.

Par ailleurs, les mesures doivent permettre d'assurer la résilience constante des systèmes et des services de traitement afin de pouvoir assurer leur maintien, notamment par la mise en place d'un plan de continuité d'activité.

S'il appartient en général à l'administration de déterminer librement les garanties appropriées pour pallier les risques inhérents à un traitement de données, certaines mesures sont expressément mises en avant par la loi et/ou revêtent une importance particulière, notamment :

- le cloisonnement et la journalisation des accès aux données ;
- la pseudonymisation des données, le cas échéant avec recours à un tiers de confiance fonctionnellement indépendant du responsable du traitement ;
- l'anonymisation des données, le cas échéant avec recours à un tiers de confiance fonctionnellement indépendant du responsable du traitement ;
- le chiffrement des données à caractère personnel en transit et au repos ;
- la sensibilisation du personnel à la protection des données et au secret professionnel.

Pour les traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées, le RGPD impose la réalisation d'une analyse d'impact relative à la protection des données (« AIPD »).

Dans le cadre de l'AIPD, le responsable du traitement doit évaluer la nécessité et la proportionnalité du traitement de données en question et minimiser les risques pour les droits et libertés des personnes concernées.

Dans l'hypothèse où le responsable du traitement ne parvient pas à identifier des mesures suffisantes pour réduire les risques à un niveau acceptable, la consultation de la CNPD quant au traitement en question est obligatoire. Cette consultation doit se faire en amont du traitement de données.

Lorsque la CNPD est d'avis que le traitement en question constituerait une violation du RGPD, elle est tenue de fournir, par écrit, un avis au responsable du traitement et, le cas échéant, au sous-traitant. Pour ce faire, elle dispose a priori d'un délai maximum de huit semaines à compter de la réception de la demande de consultation (ce délai pouvant être prolongé de six semaines, en fonction de la complexité du traitement envisagé).

LE CLOISONNEMENT ET LA JOURNALISATION DES ACCÈS AUX DONNÉES

La gestion des accès

La gestion des accès constitue une mesure permettant de réduire les risques pour les droits et libertés des personnes concernées en ce qu'elle permet d'assurer le respect des principes de minimisation des données et de limitation des finalités du traitement de données.

L'administration doit déterminer la finalité (qui doit être légitime et explicite) avant la mise en œuvre du traitement. Pour le secteur public, les finalités sont en principe définies par la loi ou doivent être rattachées aux missions légales de l'administration.

RGPD

La gestion des accès s'inscrit aussi dans une optique du respect du principe du besoin d'en connaître (principe du « need to know » au lieu du « nice to have »). Les agents ne doivent accéder qu'aux données dont ils ont besoin dans l'accomplissement de leurs tâches professionnelles, et ceci en fonction de leur rôle (« role based access control »).

La restriction des accès s'applique ainsi tant au sein d'une administration (ex. : le service « guichet » auquel parviennent les demandes de subsides ne doit en principe pas prendre connaissance des dossiers traités par le service juridique), que dans les rapports entre différentes administrations (les agents d'une administration ne doivent pas accéder aux dossiers traités par une autre administration, à moins qu'ils n'en soient habilités en vertu d'un fondement légal pour le faire).

Par exemple :

- *Le traitement de données en dehors d'une nécessité et d'une justification professionnelle est prohibé.*
- *La consultation à des fins privées des données contenues dans un fichier tenu par l'administration, tel que le registre national des personnes physiques (« RNPP »), constitue un détournement de finalité strictement interdit par la loi.*
- *Toute transmission ou divulgation de données à autrui est proscrite si le destinataire, interne ou externe à l'administration, ne remplit pas, au moment de la réception des données, les conditions dans lesquelles il est habilité à les traiter.*

La gestion des accès est un exercice qui présuppose une analyse détaillée des processus administratifs et des traitements de données effectués par l'administration.

Dans cette optique, le CTIE offre une solution standard basée sur des plateformes d'authentification et de gestion des identités (IAM), accompagnée de principes de gouvernance en termes de gestion des comptes et des accès inspirés des bonnes pratiques en la matière et garantissant une traçabilité adéquate. Cette solution facilite l'application des principes « need to know » et « need to use » et permet notamment aux administrations :

- *de gérer le cycle de vie des comptes utilisateurs, de la création à la désactivation ;*
- *d'attribuer et de retirer les droits d'accès ;*
- *de réaliser des revues des accès ;*
- *d'utiliser différents modes d'authentification en fonction de la sensibilité des données à protéger, notamment l'authentification forte pour les données les plus sensibles.*

Une gestion effective des accès se traduit par une adaptation ponctuelle des accès lors du changement d'affectation ou de cessation de fonctions d'un agent. Elle passe également par une révision périodique par l'administration des droits d'accès de l'ensemble des agents. Cela étant dit, l'agent doit informer son supérieur hiérarchique s'il constate qu'il dispose d'accès indus.

La journalisation des accès et des actions

La journalisation des accès et des actions assure la traçabilité des accès aux données et des actions effectuées. Elle constitue une bonne pratique de sécurité de l'information, sous réserve qu'il soit assuré que les données de journalisation ne puissent être modifiées ou supprimées. Elle contribue également à garantir le respect des règles de protection des données, à condition d'être soumise à des contrôles réguliers, en particulier en cas de réclamation ou pour corroborer les indices d'un accès illicite.

Dans le cadre de la journalisation des accès et des actions, une importance particulière revient à la possibilité pour chaque citoyen de vérifier sur le site Internet « MyGuichet.lu » la liste des administrations ayant consulté les données le concernant inscrites au RNPP.

Cette faculté offerte par l'article 38 de la loi du 19 juin 2013 sur l'identification des personnes physiques assure une certaine transparence à l'égard des citoyens et constitue un complément précieux au droit d'accès.

LA PSEUDONYMISATION DES DONNÉES

La pseudonymisation constitue un traitement de données réalisé de telle manière **que l'on ne puisse plus attribuer les données à une personne physique sans avoir recours à des informations supplémentaires**. Les informations supplémentaires doivent être conservées séparément et être soumises à des mesures techniques et organisationnelles afin d'éviter la ré-identification non autorisée des personnes concernées.

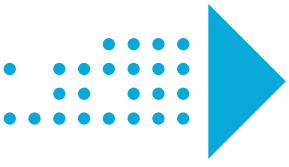
La pseudonymisation des données diminue les risques d'atteintes à la confidentialité et partant l'impact d'une telle atteinte sur les droits et libertés des personnes concernées. Elle constitue une mesure technique appropriée au sens du RGPD qui permet aux administrations de remplir leurs obligations en matière de protection des données.

La technique de la pseudonymisation a émergé du secteur de la recherche scientifique pour répondre aux besoins de mettre en relation les données initialement collectées avec des données plus récentes, voire futures, tout en offrant aux personnes concernées une certaine protection.

En pratique, la pseudonymisation **consiste à remplacer les données directement identifiantes** (ex. : numéro de matricule, nom, prénom de la personne concernée) **par un « pseudonyme »**, c'est-à-dire par un set d'informations indirectement identifiantes (alias, numéro séquentiel, etc.).

DONNÉES « EN CLAIR »

Personne concernée	Âge
Marc Schmitt	52
Carine Muller	43
Tania Weber	31



BASE DE DONNÉES PSEUDONYMISÉES

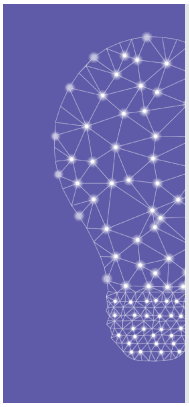
Personne concernée	Âge
1583	50-55
9856	40-45
3409	30-35

BASE DE DONNÉES D'IDENTIFICATION (CONSERVÉE À PART)

Identité	Pseudo
Marc Schmitt	1583
Carine Muller	9856
Tania Weber	3409

Contrairement à l'anonymisation, **la pseudonymisation est un processus réversible**. Pour ces motifs, **les données pseudonymisées restent des données à caractère personnel au sens du RGPD**.

Le responsable du traitement doit évaluer la pertinence du recours à la pseudonymisation en tenant compte de différents facteurs tels que la nature, la portée, le contexte et les risques inhérents au traitement, à moins que la pseudonymisation ne soit imposée par la loi.



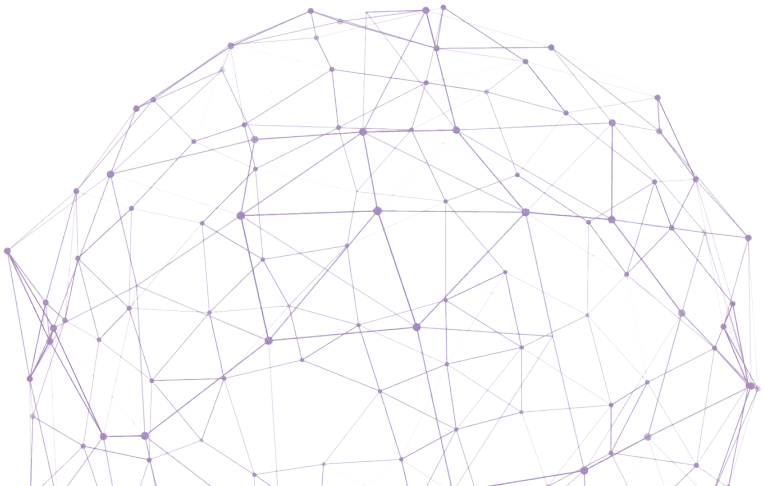
Par exemple :

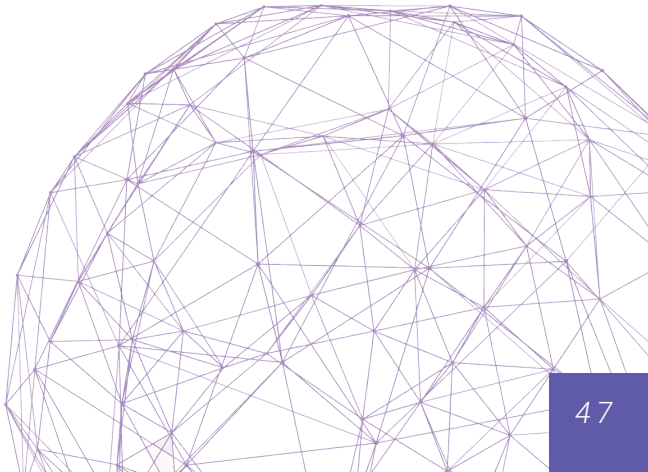
L'Inspection générale de la sécurité sociale (« IGSS ») procède à une pseudonymisation des données qu'elle centralise pour les différentes institutions de sécurité sociale en vue de la réalisation d'analyses et d'études à des fins d'évaluation des régimes de protection sociale. Elle met ces données pseudonymisées également à disposition des chercheurs pour des traitements ultérieurs de données, en particulier la réalisation d'études menées à des fins de recherche scientifique à travers une plateforme sécurisée (Microdata platform).

Sans préjudice de la possibilité pour le responsable du traitement de réaliser la pseudonymisation en interne, celle-ci peut également être effectuée par un tiers de confiance.

Le tiers de confiance est la personne physique ou morale, ou toute autre entité fonctionnellement indépendante du responsable du traitement qui pseudonymise ou anonymise les données à caractère personnel.

Compte tenu de son indépendance, le recours à un tiers de confiance constitue une garantie supplémentaire pour la sauvegarde des droits et libertés des personnes concernées dans le cadre du traitement subséquent des données.





L'ANONYMISATION DES DONNÉES

L'anonymisation des données est un processus qui consiste à utiliser un ensemble de techniques **de manière à rendre impossible toute identification** de la personne concernée par quelque moyen que ce soit, **et ce de manière irréversible**.

L'anonymisation ne se caractérise donc pas par la simple suppression de certaines données dans un fichier (ex. : le matricule, le nom, le prénom ou le numéro de compte bancaire). L'anonymisation doit, au contraire, **exclure toute possibilité de ré-identification des individus**, que ce soit à l'aide des informations détenues par l'administration, ou à l'aide d'éventuelles autres informations détenues par un tiers.

DONNÉES À CARACTÈRE PERSONNEL	DONNÉES PSEUDONYMISÉES	DONNÉES ANONYMISÉES
Jean Schmitt a un salaire annuel brut de 72 352€.	Le contribuable « 3952ZB » a un salaire annuel brut compris entre [72000€ et 75000€] (* une base de données distincte tenue par l'entité contient l'information que le pseudonyme « 3952ZB » se rapporte à Jean Schmitt.).	Un contribuable a un salaire annuel brut compris entre [72000€ et 75000€].

Les techniques d'anonymisation sont multiples. Elles comprennent notamment :

- *la généralisation du jeu de données (ex. : remplacement de l'information sur la « nationalité » par l'information « ressortissant de l'Union européenne ») ;*
- *la randomisation des attributs dans un jeu de données (ex. : altération de la véracité de certaines informations dans le jeu de données sans que cela n'affecte la pertinence de l'information).*

Certaines informations, prises isolément, ne contiennent pas – directement ou indirectement – d'indications sur l'identité d'un individu. Or, cela ne signifie pas forcément que ces informations sont à considérer comme des « informations anonymisées ».

Les informations restent des données à caractère personnel au sens du RGPD si leur combinaison avec d'autres informations permet d'identifier la personne concernée de manière univoque.

Exemples :

Un sondage par questionnaire auprès de certains agents d'une administration pourrait, même en l'absence d'indication des noms et prénoms, contenir des informations qui, combinées les unes aux autres, permettent de révéler l'identité de la personne concernée (ex. : 38 ans, femme, économiste, entrée en service en mai 2016).

Une facture, contenant un numéro de référence ainsi que les coordonnées de la société venderesse, collectée et traitée par une administration dans le cadre de l'examen d'une demande de subside constitue une donnée à caractère personnel au sens du RGPD. En effet, même si elle ne renseigne pas les coordonnées de l'acquéreur (c'est-à-dire du demandeur du subside), elle permet potentiellement de ré-identifier la personne concernée, notamment grâce aux informations détenues par des tiers (ex. : la société venderesse ou l'institut bancaire).

En pratique, il est difficile d'« anonymiser » une information de manière à pouvoir exclure toute ré-identification potentielle des individus. De nombreux travaux de recherche démontrent que la ré-identification devient de plus en plus facile du fait de la multiplicité des données disponibles, de leur degré de précision et des techniques informatiques de recoupement de données, y compris à l'aide de solutions d'intelligence artificielle.

Pour vérifier si une information peut effectivement être considérée comme « anonymisée », il convient d'après les autorités de protection des données européennes de tenir compte, en particulier, des critères suivants :

1

L'individualisation, qui vise la possibilité d'isoler un individu dans ledit jeu de données sur base des informations y contenues.

Par exemple :

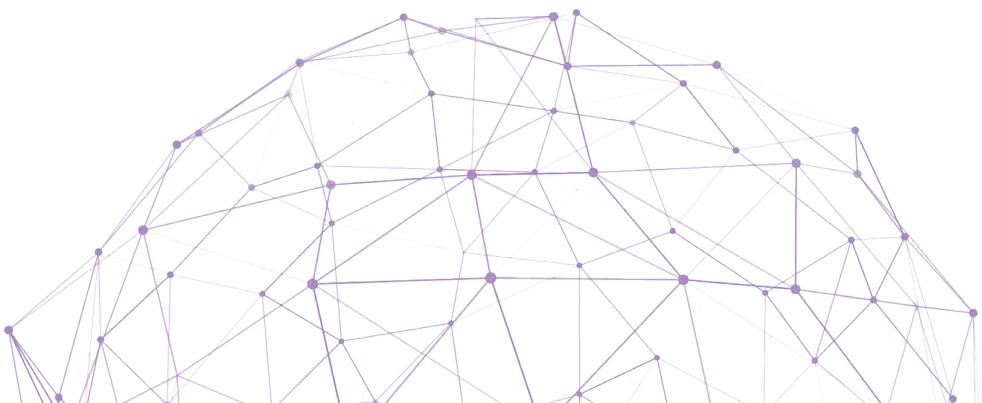
Si les numéros de matricule, les noms et les prénoms des individus listés dans un fichier tenu par l'administration sont remplacés par un identifiant unique tel qu'un numéro client, le fichier sera considéré comme contenant des informations « pseudonymisées » et non pas des informations « anonymisées ».

La corrélation, qui vise la possibilité de combiner, d'interconnecter ou de relier des sets de données distincts, que ce soit au sein des systèmes d'information d'une même administration ou d'administrations différentes.

2

Par exemple :

Une base de données géographiques contenant des informations sur les rapports de propriété et les parcelles de terrain, notamment à l'aide de numéros ou d'identifiants, ne saurait être considérée comme « anonymisée » si d'autres bases de données contiennent ces mêmes numéros ou identifiants ensemble avec d'autres informations permettant d'identifier les personnes concernées.



3 **L'inférence,** qui vise la possibilité de déduire avec une certitude suffisante, de nouvelles informations sur la personne concernée.

Par exemple :

Une enquête concernant les maladies génétiques, basée sur les réponses fournies par les membres d'un groupe sélectionné à un questionnaire « anonyme » ne saurait être considérée comme telle, dès lors que tous les participants de sexe masculin entre 20 et 30 ans ont indiqué ne pas souffrir d'une telle maladie, sauf un individu qui s'avère être le seul ressortissant d'un pays tiers. Dans ce cas de figure, il sera possible de déduire sans équivoque que Monsieur X., 28 ans et ressortissant d'un pays tiers, est la personne souffrant d'une maladie génétique.

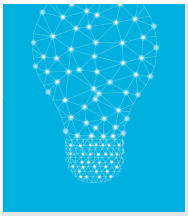
Ainsi, si un set de données permet, notamment, l'individualisation, la corrélation ou l'inférence, il ne peut être considéré comme « anonymisé ».

Dans une optique d'« accountability », l'administration responsable du traitement doit régulièrement s'assurer que les techniques d'anonymisation employées sont effectives. Elle est tenue d'effectuer une veille desdites mesures afin de préserver, dans le temps, le caractère anonyme des informations tout en tenant compte des moyens techniques disponibles qui permettent de lever l'anonymat.

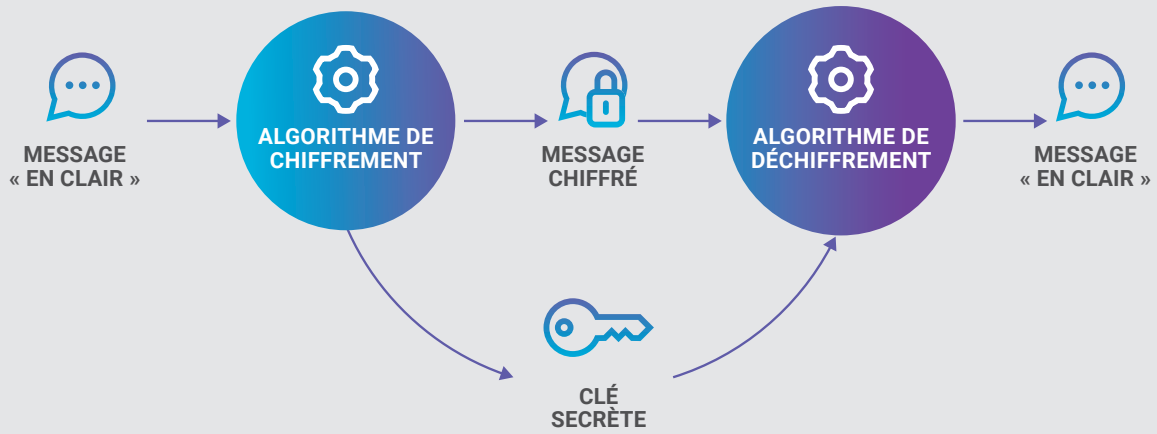
LE CHIFFREMENT DES DONNÉES

Le chiffrement permet de réduire le risque d'atteinte à la sécurité de l'information en ce qu'il rend les données incompréhensibles en transformant un message « en clair » en un message « chiffré ».

Seules les personnes habilitées disposeront de la clé de déchiffrement donnant accès au contenu sous une forme intelligible. La sauvegarde et la transmission de la clé doivent se faire de manière sécurisée, compte tenu de l'état de connaissance et des coûts de mises en œuvre (ex. : ne pas communiquer la clé par le même canal que celui du document chiffré).

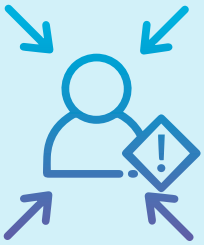


Le chiffrement d'un message est comparable à une enveloppe numérique scellée : une fois chiffré, le message devient inaccessible et illisible aux personnes ne possédant pas la clé spécifique de chiffrement/de déchiffrement.



LA SENSIBILISATION DU PERSONNEL

L'individu est l'un des maillons faibles de la sécurité de l'information et des données.



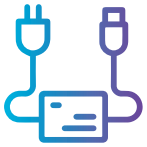
D'après la CNPD,

62 %

des violations de données en 2021 ont été causées par une erreur humaine (acte interne non malveillant).

Il existe **un large éventail d'erreurs humaines** susceptibles de porter atteinte à la sécurité des informations et des données, notamment :

L'ENVOI D'UN MAIL AU MAUVAIS DESTINATAIRE



L'UTILISATION D'ÉQUIPEMENTS PERSONNELS (EX. : IMPRIMANTE, CLÉ USB) NON SÉCURISÉS

L'OUBLI DE DOCUMENTS CONFIDENTIELS (EX. : DANS L'IMPRIMANTE, LA PHOTOCOPIEUSE OU SUR LE BUREAU)

L'OUVERTURE DE MAILS MALVEILLANTS

LE TÉLÉCHARGEMENT D'ÉLÉMENTS CORROMPUS (EX. : FICHIERS, LOGICIELS)

L'UTILISATION DE SOLUTIONS DE PARTAGE DE FICHIERS NON VALIDÉES PAR L'ADMINISTRATION PUBLIQUE (EX. : RÉSEAUX SOCIAUX)

LA COMMUNICATION D'INFORMATIONS À DES PERSONNES SANS VÉRIFICATION PRÉALABLE DE LEUR IDENTITÉ ET HABILITATION

LE PARTAGE DE SON ORDINATEUR PROFESSIONNEL AVEC DES TIERS (EX. : MEMBRES DE LA FAMILLE)

LE CHOIX DE MOTS DE PASSE TROP FAIBLES OU FACILEMENT DEVINABLES

L'administration doit promouvoir une culture de la sécurité de l'information et des données et veiller à ce que ses agents soient sensibilisés de manière adéquate, en particulier, quant :

- aux bonnes pratiques applicables en la matière,
- à la sensibilité des données auxquelles ils ont accès,
- aux types de cyberattaques les plus courantes,
- aux acteurs internes et externes compétents en la matière,
- à la classification interne des données et des méthodes de transmission sécurisées à utiliser.

À noter que le HCPN-ANSSI a pour mission de promouvoir la sécurité de l'information par le biais de mesures de sensibilisation. Il se tient à disposition de l'ensemble des administrations et services de l'Etat pour établir conjointement un programme de sensibilisation de leurs agents.

Les acteurs publics impliqués dans le domaine de la sécurité de l'information et des données offrent des formations spécifiques en collaboration avec l'Institut national d'administration publique (« INAP »). En outre, ils publient régulièrement des documents de guidance et de sensibilisation (affiches, lignes directrices, modèles et guides pratiques) pour assister les administrations dans cet exercice.

Citons, à titre d'illustration :

- *l'espace de partage d'informations et de documents du CGPD,*
- *le portail interactif du CTIE « LogON CTIE » (pour les administrations étatiques qui recourent aux services et outils informatiques du CTIE),*
- *l'extranet de l'ANSSI (pour les administrations et services de l'Etat).*

SECTION 4 :
L'AGENT AU CENTRE DE LA SÉCURITÉ DE L'INFORMATION ET DES DONNÉES

Les obligations de l'agent

L'agent est tenu de se conformer consciencieusement aux lois et règlements qui encadrent l'exercice de ses fonctions, aux instructions du gouvernement qui ont pour objet l'accomplissement régulier de ses devoirs ainsi qu'aux ordres de service de ses supérieurs (loi modifiée du 16 avril 1979 fixant le statut général des fonctionnaires de l'Etat).

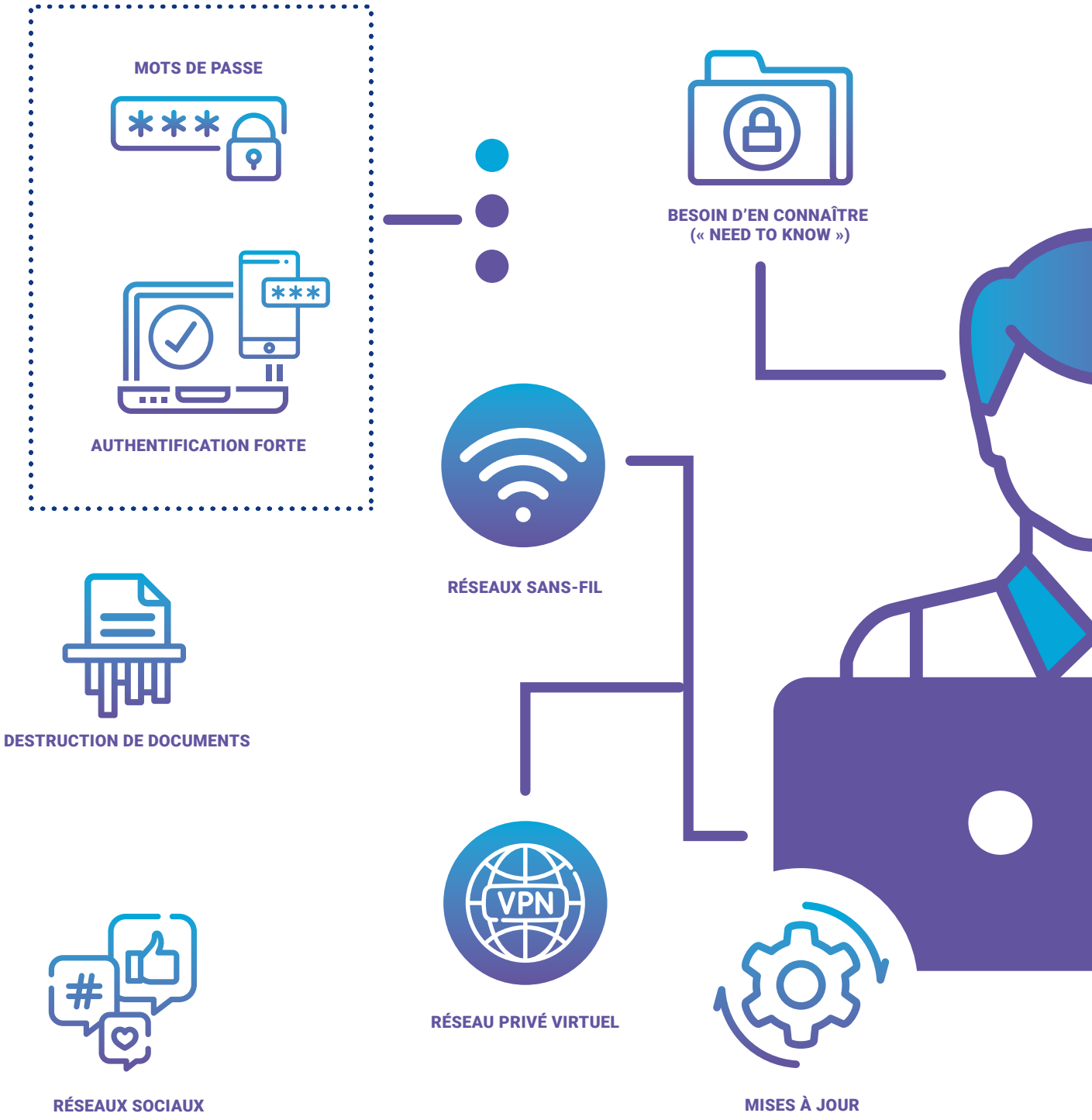
L'agent a **une obligation de discrétion et de secret professionnel**. Il ne doit pas révéler les faits dont il a obtenu connaissance en raison de ses fonctions et qui auraient un caractère secret de par leur nature ou de par les prescriptions de ses supérieurs hiérarchiques, à moins d'en être dispensé par le ministre du ressort.

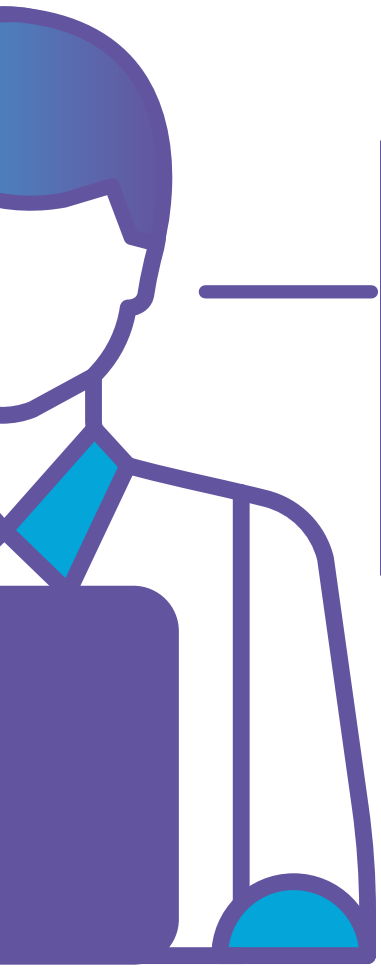
De ce fait, toute transmission ou divulgation de données est proscrite si le destinataire (interne ou externe à l'administration) ne remplit pas, au moment de la réception des données, les conditions dans lesquelles il est habilité à les traiter.

En outre, **l'agent doit traiter les données dans les strictes limites des missions d'intérêt public poursuivies par l'administration et pour les seuls objectifs fixés par celle-ci. Tout détournement et toute communication à des tiers contraires aux lois et règlements sont interdits.**

Les bonnes pratiques à respecter par l'agent

L'agent doit mettre en œuvre des bonnes pratiques en matière de sécurité de l'information et de sécurité des données à caractère personnel. Celles-ci sont illustrées à l'aide de ce graphique et décrites plus en détail dans la présente section.





VIDÉOCONFÉRENCES

APPELS TÉLÉPHONIQUES

MESSAGERIE ÉLECTRONIQUE

« CLEVER CLICKS »

« BRING YOUR OWN DEVICE »

DÉPLACEMENTS PROFESSIONNELS

SÉCURITÉ DES LOCAUX DE L'ADMINISTRATION

TÉLÉTRAVAIL

POLITIQUE DU BUREAU PROPRE ET DE L'ÉCRAN VERROUILLÉ (« CLEAN DESK POLICY »)

CONTACTER LES SERVICES COMPÉTENTS EN CAS DE QUESTIONS OU DE DOUTES

Les mots de passe

L'authentification par « noms d'utilisateur » et « mots de passe » est le moyen le plus simple et le moins coûteux pour contrôler un accès, notamment à un ordinateur ou une application, et pour prouver l'identité de l'utilisateur.

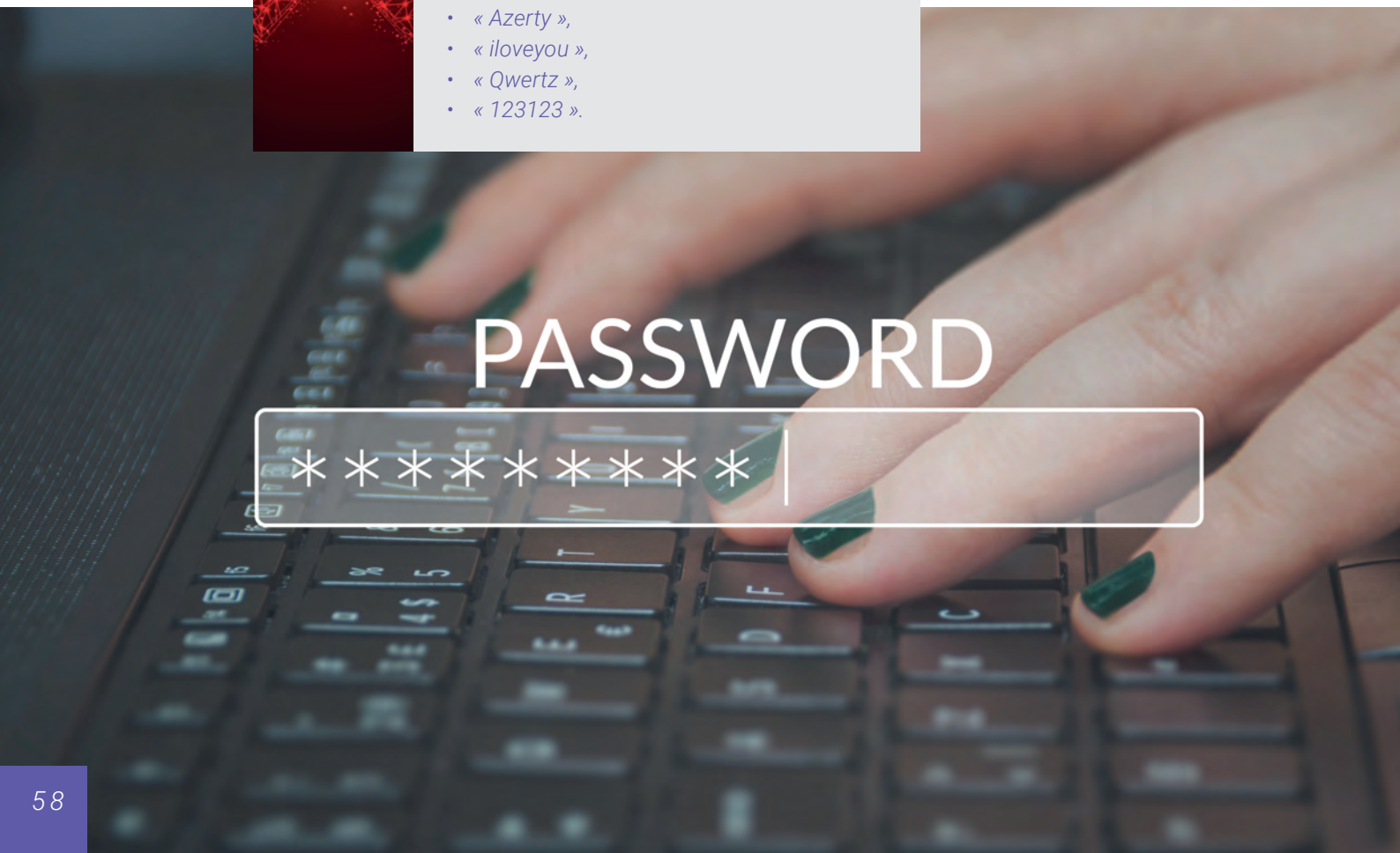
L'avantage de ce moyen d'authentification réside dans sa simplicité ainsi que dans le fait que la grande majorité des agents sont familiers avec cette mesure de sécurité.

Néanmoins, le recours aux mots de passe présente également des inconvénients :

- les mots de passe peuvent facilement être copiés ou observés à l'insu de l'utilisateur (ex. : attaques d'hameçonnage (« phishing ») ou regards par-dessus l'épaule des utilisateurs (« shoulder surfing »)) ;
- beaucoup d'utilisateurs emploient des mots de passe courants ou des mots de passe faciles à deviner (ex. : « 123456 », « Password » ou « QWERTY ») ;
- les individus utilisent un mot de passe unique pour plusieurs applications.

D'après les acteurs spécialisés en sécurité de l'information, figurent parmi les mots de passe les plus répandus :

- *« password »,*
- *« 123456 »,*
- *« 123456789 »,*
- *« Guest »,*
- *« QWERTY »,*
- *« abc123 »,*
- *« Azerty »,*
- *« iloveyou »,*
- *« Qwertz »,*
- *« 123123 ».*



Afin de minimiser les risques d'usurpation, il importe de choisir un mot de passe « fort » en respectant quelques règles essentielles :

1

Utiliser des mots de passe distincts pour des usages distincts.

L'**utilisation de mots de passe distincts** permet d'éviter les piratages en cascade. Ainsi, en cas de vol ou de perte du mot de passe, seule l'application ou seul le compte concerné sera vulnérable.

La Charte de bonne conduite en matière de sécurité de l'information numérique de l'ANSSI interdit la réutilisation de mots de passe personnels attachés à des comptes privés pour accéder aux systèmes d'information de l'Etat.

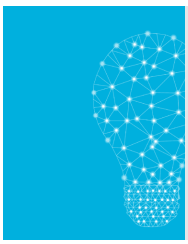
Utiliser un mot de passe suffisamment long et complexe, impossible à deviner.

2

Pour pouvoir résister à des attaques « force brute », le mot de passe doit être suffisamment long et complexe. D'après les bonnes pratiques actuelles, il doit être **composé d'au moins 12 caractères et comprendre à la fois des minuscules, des majuscules, des chiffres et des caractères spéciaux.**

L'attaque par « force brute » consiste à essayer toutes les combinaisons possibles de caractères jusqu'à trouver le mot de passe de l'utilisateur. Compte tenu des avancées techniques (utilisation de solutions d'intelligence artificielle), des dizaines de milliers de combinaisons par seconde peuvent être testées à l'occasion de ces attaques.

Par ailleurs, l'agent doit **éviter le recours aux mots du dictionnaire, aux suites logiques** (ex. : « 123456 » ou « QWERTZ ») **ainsi qu'aux informations personnelles** (ex. : le prénom de son enfant, son club de sport préféré, sa plaque d'immatriculation, sa date de naissance).



L'attaque par « dictionnaire » consiste à tester automatiquement tous les mots contenus dans les dictionnaires d'une langue donnée. Elle est basée sur l'hypothèse que l'agent a créé son mot de passe en utilisant un terme défini dans un tel dictionnaire. Compte tenu de l'avancement des technologies, ce type d'attaque permet de démasquer un mot de passe en quelques secondes.

Pour ces motifs, il est recommandé à l'agent de choisir son mot de passe en utilisant la technique de la « phrase » (« méthode des premières lettres ») ou la technique « phonétique », tout en respectant les conditions des caractères spéciaux (ex. : « @ », « ! » ou « & »), des chiffres, des minuscules ainsi que des majuscules.

Exemple d'un mot de passe par la technique de la « phrase » :

- *phrase à retenir : « deux vaches et un cheval sur le toit se posent trois questions »,*
- *mot de passe : « 2V&1Csltsp3? ».*

Exemple d'un mot de passe par la technique « phonétique » :

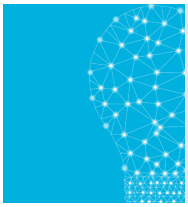
- *phrase à retenir : « : j'ai acheté huit cd pour cent euros cet après-midi »,*
- *mot de passe : « Ght8CD%E7ami ».*

3

Ne pas partager un mot de passe et ne pas le divulguer à des tiers.

Le mot de passe **doit rester secret** en toute circonstance. Ainsi, l'agent ne doit jamais :

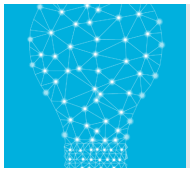
- demander à un tiers de générer son mot de passe ;
- partager son mot de passe avec d'autres personnes, y compris dans le cadre d'une utilisation commune de la même application informatique ;
- conserver son mot de passe en clair, que ce soit sous format électronique ou papier (ex. : mention du mot de passe sur un post-it collé sur l'écran, annotation du mot de passe au dos du clavier, envoi à soi-même du mot de passe par mail) ;
- divulguer son mot de passe à des tiers.



Ni le CTIE, ni le GOVCERT, ni le RSSI ou le DPD de l'administration ne demanderont à l'agent de communiquer le mot de passe par mail ou par téléphone. De ce fait, l'agent ne doit pas répondre à de telles demandes, car il s'agirait probablement d'une tentative d'extorsion de mot de passe.

Changer son mot de passe régulièrement.

L'agent doit changer son mot de passe régulièrement afin de réduire les risques de piratage.



A cette fin, le CTIE envoie à intervalles réguliers des messages informant les agents que leur mot de passe actuel arrivera à expiration au terme du délai communiqué et les invite à le renouveler.

4

Dans ce même ordre d'idées, l'utilisateur doit changer son mot de passe au moment de la première connexion lorsque celui-ci a été généré par défaut par le gestionnaire des équipements et des solutions informatiques.

Toutefois, pour que le changement du mot de passe à une fréquence régulière constitue une mesure réellement efficace, il convient de ne pas seulement modifier légèrement le mot de passe précédent, notamment en ajoutant ou modifiant un chiffre à la fin. A défaut, les bénéfices du changement de mot de passe en termes de sécurité seraient mineurs.

5

Changer son mot de passe immédiatement en cas de compromission réelle ou suspectée.

Dans l'hypothèse où l'agent suspecte une compromission de son mot de passe, il doit le changer immédiatement afin d'éviter des utilisations illicites par des tiers (sans préjudice de l'obligation d'alerter au plus tôt les services compétents).

Ne pas utiliser de gestionnaire de mots de passe sur Internet.

6

La Charte de bonne conduite en matière de sécurité de l'information numérique de l'ANSSI interdit l'utilisation de gestionnaires de mots de passe sur Internet, tout en recommandant, en cas de besoin, l'utilisation d'un coffre-fort numérique (ex. : Keepass) pour le stockage sécurisé et chiffré des mots de passe.

7

Ne pas laisser son navigateur ou une application mémoriser le mot de passe.

De nombreux logiciels, dont les navigateurs, offrent la possibilité de sauvegarder les mots de passe des utilisateurs afin de ne plus devoir les saisir. Malgré son aspect pratique, cette option emporte des risques substantiels en termes de sécurité de l'information.

Pour ces motifs, la Charte de bonne conduite en matière de sécurité de l'information numérique de l'ANSSI n'autorise pas la mémorisation de mots de passe dans les navigateurs Internet, mais recommande l'utilisation d'un coffre-fort numérique.

Ne pas tenter de contourner les systèmes d'authentification et d'accéder à des systèmes d'information avec les identifiants d'un autre utilisateur.

8

Il est interdit à l'agent d'essayer de contourner les systèmes d'authentification et d'accéder à des systèmes d'information avec les identifiants d'un autre utilisateur. De tels actes risquent de compromettre la sécurité des systèmes d'information et des données et d'exposer l'agent à d'éventuelles sanctions disciplinaires voire, le cas échéant, pénales.

L'authentification forte

Les méthodes d'authentification à plusieurs facteurs (« authentification forte ») offrent une protection renforcée par rapport à la méthode d'authentification par mot de passe.

L'authentification forte consiste en l'**utilisation d'au moins deux facteurs d'authentification** distincts, correspondant, en particulier :

À DES INFORMATIONS CONNUES PAR L'UTILISATEUR (EX. : MOT DE PASSE OU CODE PIN)

À UN OBJET QUE L'UTILISATEUR POSSÈDE (EX. : « SMARTCARD LUXTRUST »)

À UN ÉLÉMENT SPÉCIFIQUE DE L'UTILISATEUR (EX. : EMPREINTE DIGITALE OU RECONNAISSANCE FACIALE)

La multiplicité des facteurs d'authentification assure qu'un tiers ne puisse accéder au compte d'utilisateur dans l'hypothèse où il parviendrait à se procurer le mot de passe de l'agent, faute de disposer du second facteur d'authentification. Bien que l'utilisation de l'authentification forte n'empêche pas tous les types d'attaques, elle rend plus difficile le piratage du compte de l'agent.

Pour que cette mesure soit efficace, l'agent doit veiller à ne pas divulguer ses identifiants et respecter les bonnes pratiques applicables en la matière.

Dans le cadre de l'utilisation de la « SmartCard Luxtrust » (moyen d'authentification forte le plus courant dans les administrations étatiques et communales), il faut, en particulier :

- *choisir un code PIN complexe et non devinable,*
- *ne pas conserver son code PIN ensemble avec la SmartCard,*
- *ne pas partager son code PIN ou sa SmartCard avec un tiers,*
- *ne pas laisser la SmartCard dans le lecteur de carte de son ordinateur après utilisation.*

« Bring your own device »

La notion de « Bring your own device », aussi connue sous l'acronyme « BYOD », décrit la situation dans laquelle les agents apportent leur matériel personnel (ex. : téléphone, tablette) dans l'environnement professionnel et l'utilisent tant à des fins privées qu'à des fins professionnelles.

Le phénomène du BYOD, bien que constituant une ouverture pratique pour l'utilisateur, comporte des risques en termes de sécurité de l'information, notamment dû au fait que les équipements privés risquent de ne pas être protégés de manière aussi sécurisée que les ressources informatiques gérées par les administrations.

Pour cette raison, **l'utilisation du BYOD est strictement encadrée par le CTIE**, à savoir notamment par la Charte d'accès à la messagerie de l'Etat avec un équipement mobile privé (BYOD) et le Guide des bonnes pratiques en matière de la sécurité d'information mobile.

En outre, l'accès au réseau de l'Etat est réservé aux équipements autorisés, gérés et mis à disposition par les services compétents. La connexion d'équipements privés ou d'équipements visiteurs, qu'elle soit filaire ou sans fil, au réseau de l'Etat est interdite. Cette restriction ne s'applique évidemment pas aux réseaux dédiés à la connexion de terminaux personnels ou visiteurs.

A noter que l'agent doit en tout état de cause s'abstenir de prendre en photo ou vidéo des documents ou des informations professionnels non publics avec ses équipements privés (ex. : smartphone). De même, il lui est interdit d'enregistrer les paroles d'autrui, à moins d'avoir obtenu le consentement préalable des personnes concernées ou d'être habilité par ou en vertu de la loi.

Le réseau privé virtuel (« VPN »)

L'usage du VPN permet aux agents de travailler en dehors des locaux de l'administration tout en accédant de manière sécurisée au réseau interne de celle-ci.

Un VPN est un moyen de communication assurant la sécurité des transferts de données sur des réseaux publics ou partagés. Il s'agit d'une technologie permettant l'extension logique du réseau, par l'ajout de postes ou sous-réseaux se trouvant à l'extérieur des limites physiques de celui-ci. Grâce à des mécanismes cryptographiques, le canal VPN s'apparente à un tunnel virtuel ne contenant que des données chiffrées non-modifiables.

Compte tenu du fait que l'accès à distance aux ressources informatiques internes de l'Etat et des communes est réservé aux personnes ayant le besoin métier, l'agent travaillant à distance et se connectant à des ressources informatiques pour des besoins professionnels doit :

- disposer d'une autorisation formelle de sa hiérarchie ;
- n'utiliser que le matériel fourni, à savoir un moyen de connexion spécifiquement configuré à ces fins et sécurisé ;
- veiller à ce que le matériel fourni pour le télétravail ou l'accès à distance ne soit pas utilisé par un tiers ;
- ne pas contourner ou tenter de contourner les mesures et dispositifs de sécurité permettant d'assurer une connexion sécurisée à distance.

La Charte de bonne conduite en matière de sécurité de l'information numérique de l'ANSSI rappelle que chaque utilisateur accédant au VPN de l'Etat est personnellement responsable de l'utilisation qu'il en fait.

Réseaux sans-fil (Wifi)

L'agent doit veiller à ce que la connexion au réseau sans-fil (« Wifi ») ne nuise pas à la sécurité de l'information de l'administration.

De ce fait, il doit dans le cadre de ses activités professionnelles éviter au maximum l'utilisation de réseaux Wifi non gérés par l'administration.

Par ailleurs, en cas de connexion à un réseau Wifi à des fins professionnelles, l'agent doit :

- n'activer l'interface Wifi que lorsque celle-ci doit être utilisée,
- éviter de se connecter à des réseaux sans-fil non sécurisés (ex. : Wifi d'hôtel, de gare ou de café),
- recourir aux solutions VPN prévues par le gestionnaire informatique,
- s'assurer que le pare-feu et l'antivirus sont activés,
- choisir une authentification forte lors d'une connexion à une application,
- désactiver le réseau sans-fil à la fin de l'utilisation,
- désactiver la connexion automatique aux points d'accès Wifi déjà utilisés.

Les exigences relatives à la connexion Wifi s'appliquent également lors de l'utilisation d'un réseau filaire inconnu ou non sécurisé (branchement au câble « Ethernet »).

L'agent doit également s'abstenir de consulter tout site Internet à risque pour la sécurité de l'information, notamment en termes d'intrusion dans les systèmes (ex. : exécution de virus, prise de contrôle à distance).

Les acteurs spécialisés en la matière, tel que le CTIE, restreignent l'accès à certains sites Internet à risque.

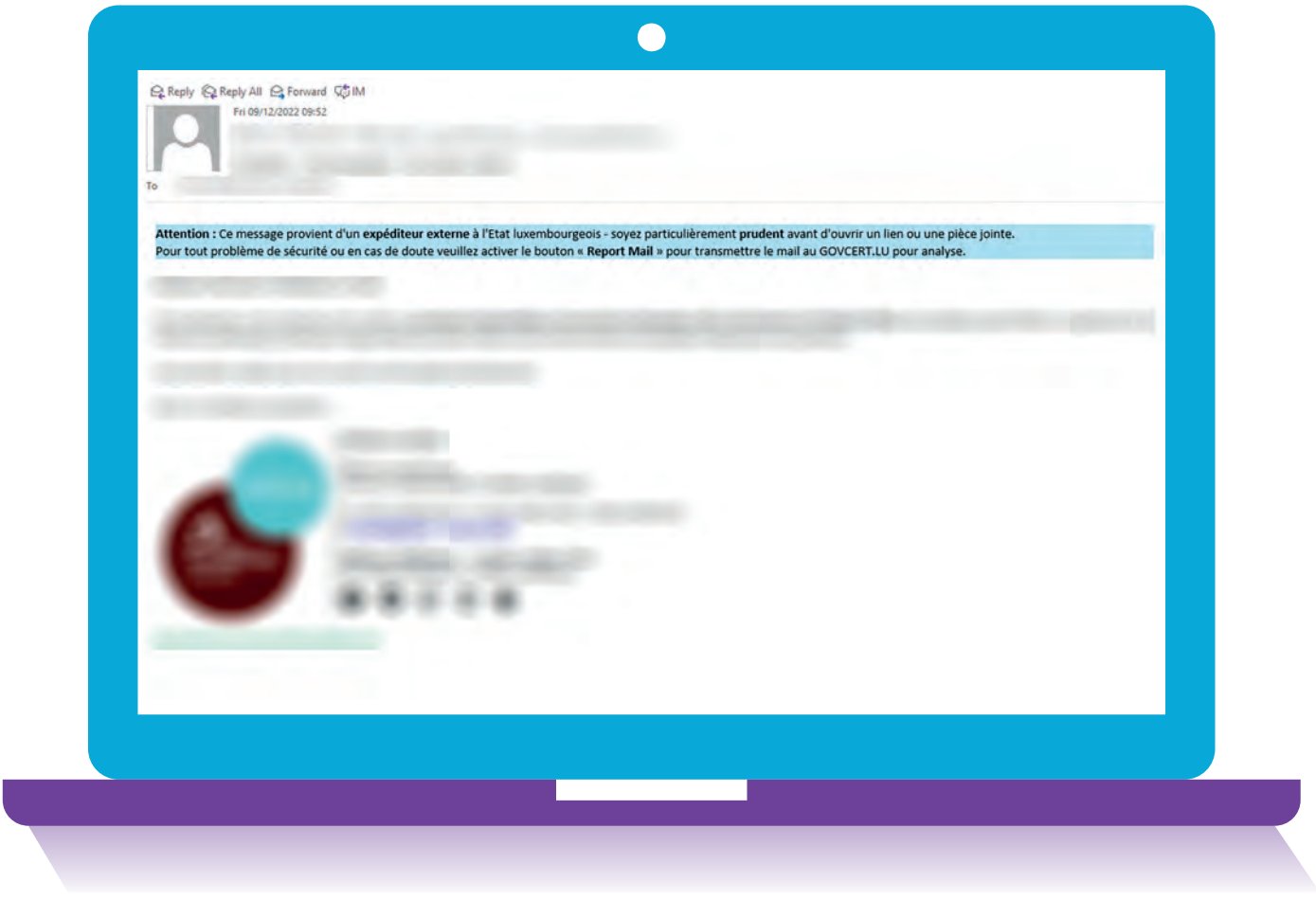
Messagerie électronique

Le mail est la principale forme de communication professionnelle de l'agent. Son utilisation nécessite une vigilance accrue de l'agent, tant au niveau de l'expédition que de la réception d'un message.

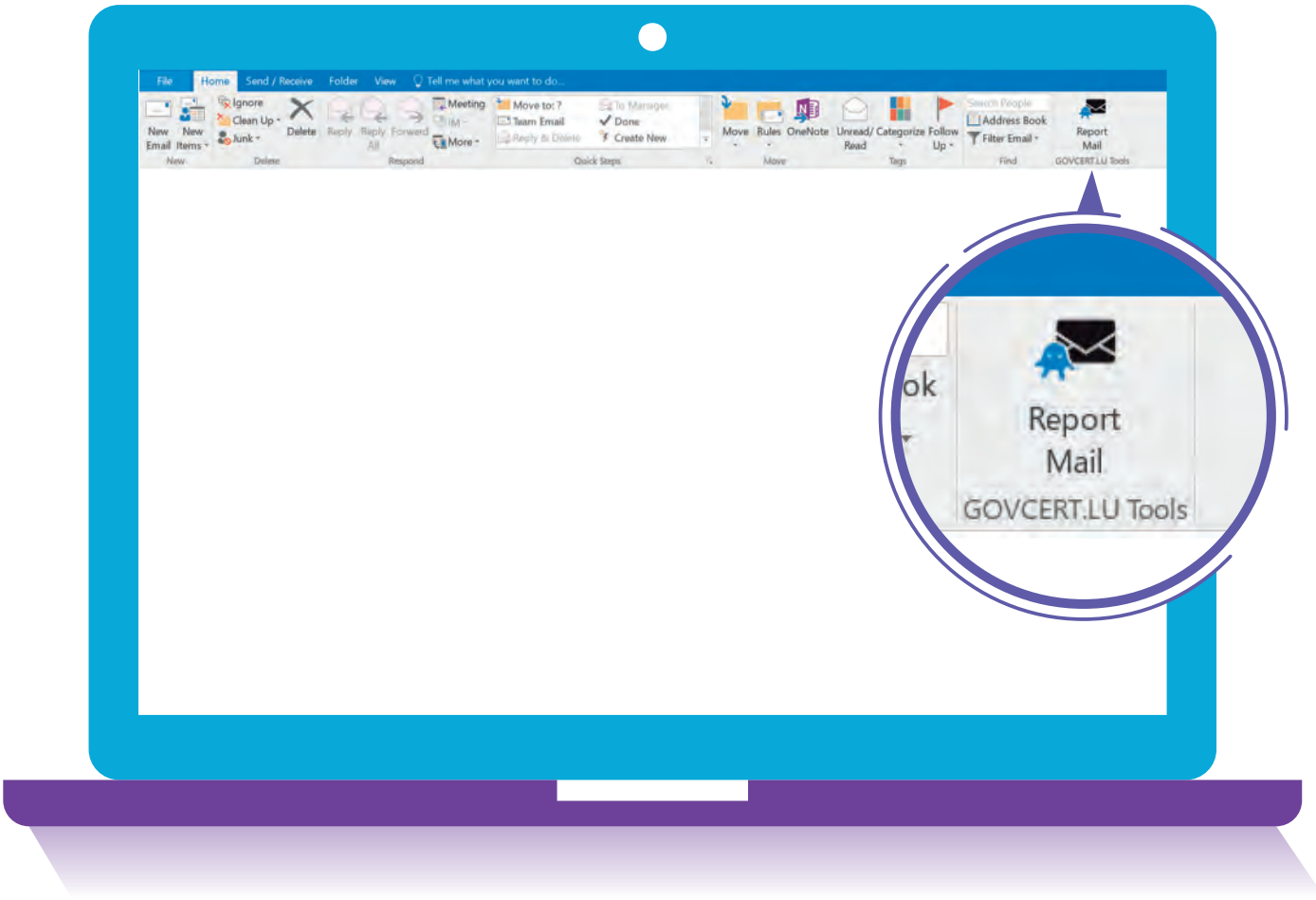
Pour ces raisons, l'agent doit, en particulier :

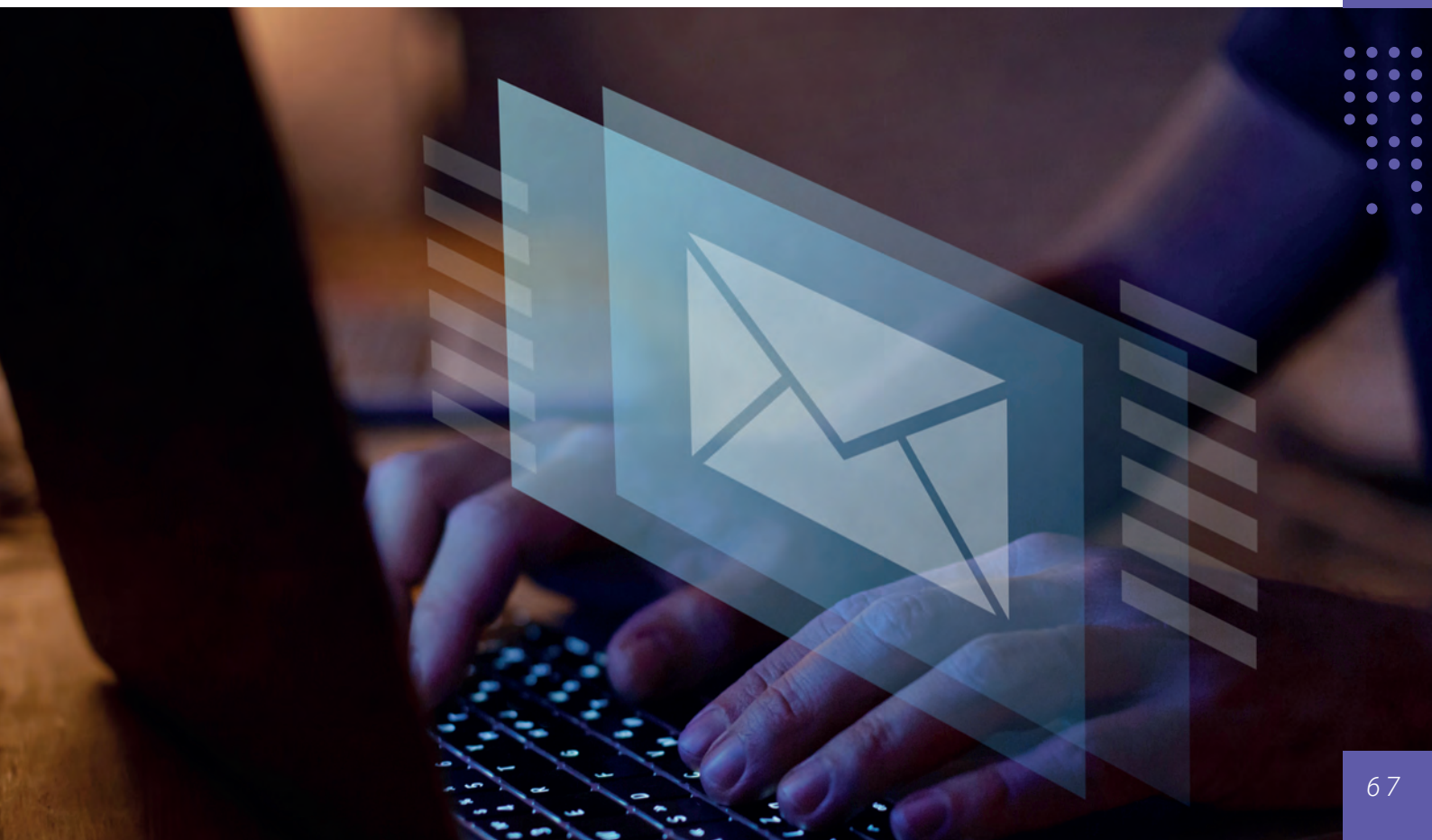
- être conscient du fait que l'acheminement, l'authenticité et l'intégrité des messages véhiculés par Internet ne sont pas garantis. Il doit faire preuve de vigilance lorsqu'il reçoit un mail avec une pièce-jointe ou contenant un lien vers un site Internet, surtout si celui-ci est de provenance inconnue ou douteuse.

Le CTIE a inséré une bannière d'information dans les mails en provenance de sources non-étatiques. L'objectif étant d'attirer l'attention des agents sur le risque qu'un tel mail externe puisse être potentiellement frauduleux et sur la nécessité, pour l'agent, de le traiter avec les précautions nécessaires.



- transmettre au GOVCERT les mails suspicieux (ex. : soupçon d'attaque « phishing ») en utilisant la fonction « Report Mail » dans sa messagerie électronique.





- s'abstenir de transférer des mails ou documents professionnels vers des adresses mails privées, qu'il s'agisse de la sienne ou celles de tiers non autorisés (ex. : membre de sa famille).

Cette interdiction vise par exemple le transfert de documents professionnels vers une adresse mail privée à des fins d'impression de documents en télétravail en ayant recours au matériel informatique privé.

- recourir à des moyens de chiffrement adéquats, fournis par le gestionnaire informatique de l'administration, en cas de transmission d'informations confidentielles.

Exemple :

L'application « One-Time-Exchange » (« OTX ») permet à un agent d'échanger des fichiers électroniques avec des personnes tierces via un canal sécurisé. La notification d'un envoi de fichier ou d'une demande de fichiers est transmise par mail. L'agent peut ensuite accéder aux documents via l'application Web OTX. Le fichier transmis reste disponible pour le destinataire durant une période définie.

- s'assurer de la confidentialité des données communiquées par mail en vérifiant notamment la légitimité des destinataires et des pièces jointes. En effet, une simple erreur ou négligence peut conduire au transfert de données à des tiers non habilités et partant à un incident de sécurité de l'information.

Dans certains cas de figure, l'envoi de messages groupés à plusieurs destinataires doit se faire sans divulguer les adresses mail des destinataires (ex. : en utilisant la fonction « Cci »). Il convient également de s'assurer que chaque destinataire est bien autorisé à recevoir les informations contenues dans le mail.

- s'abstenir d'utiliser sa boîte mail comme un espace de stockage, en particulier pour les données qui peuvent paraître sensibles (ex. : les fiches de rémunération).

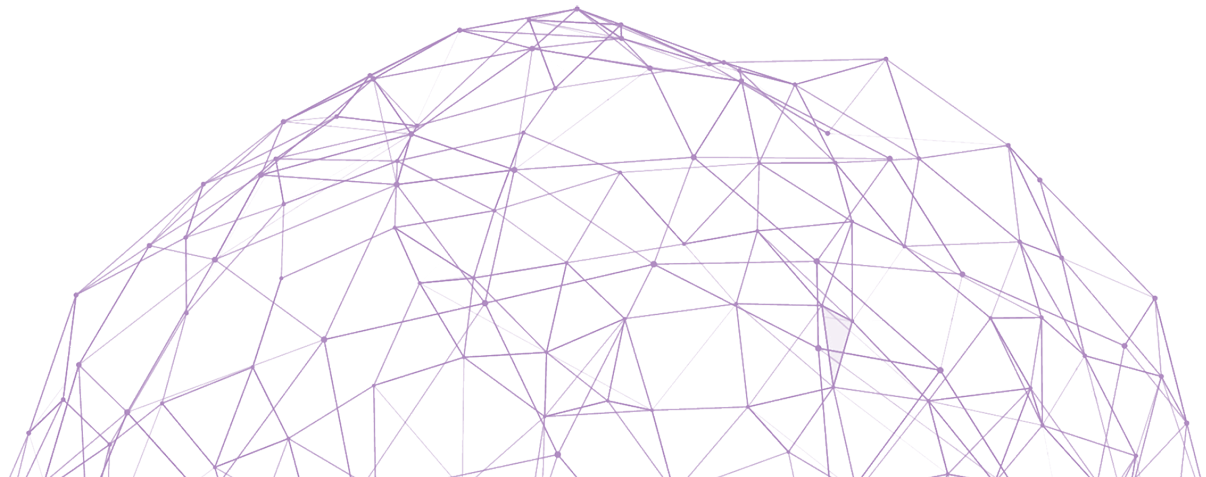
Réseaux sociaux

L'agent ne doit pas partager des informations professionnelles non publiques via les réseaux sociaux, les applications et les services de messageries instantanées qui ne sont pas gérés par l'administration publique (ex. : Facebook, Twitter, Instagram,TikTok, WhatsApp).

Compte tenu du fait que ces outils ne sont pas contrôlés par les administrations, leur installation et utilisation sur les équipements professionnels comportent des risques en termes de sécurité de l'information et de partages illicites de données avec des tiers. De ce fait, elles sont déconseillées. En tout état de cause, une utilisation de services en ligne commerciaux non contrôlés par l'administration publique ne doit se faire qu'avec précaution et retenue.

La Charte de bonne conduite en matière de sécurité de l'information numérique de l'ANSSI précise que l'utilisation des réseaux sociaux doit se faire selon les règles de bonne conduite et d'éthique.

L'agent doit être conscient des risques associés à l'utilisation de ces services et s'abstenir, en particulier, de publier des informations professionnelles non publiques via ces canaux.



Les déplacements professionnels

Dans le cadre de ses fonctions, l'agent peut être amené à effectuer des déplacements professionnels. Il devra alors faire preuve d'une vigilance accrue notamment quant aux équipements informatiques et aux informations professionnelles qu'il transporte en dehors des locaux de l'administration.

L'agent doit s'assurer, en particulier, des points suivants :

Avant le déplacement :

- prévoir d'accéder aux informations à distance de façon sécurisée (ex. : par le biais d'un site sécurisé ou d'un VPN) ;
- n'emporter que les informations nécessaires à l'accomplissement de sa mission ;
- s'assurer que les données emportées sont sauvegardées sur un support conservé au sein de l'administration ;
- protéger adéquatement les informations confidentielles emportées (ex. : utilisation de supports de stockage chiffrés).

Au cours du déplacement :

- conserver et transporter les équipements et les informations de manière sécurisée (ex. : ne pas laisser l'ordinateur portable de manière visible dans une voiture ou sans surveillance dans un espace public) ;
- faire preuve de discrétion et ne pas consulter des documents professionnels en présence de personnes non autorisées (ex. : ne pas discuter à haute voix de dossiers professionnels en présence de tiers non autorisés, notamment au cours de déplacements en train ou avion) ;
- éviter la connexion à des réseaux, des systèmes informatiques et des équipements non sécurisés ;
- prévenir au plus vite ses supérieurs hiérarchiques et les services compétents (ex. : CTIE, GOVCERT, le RSSI de l'administration et le DPD) en cas de perte ou de vol de matériels ou d'informations.

Après le déplacement :

- détruire les documents dont l'administration n'a plus besoin (sans préjudice des dispositions de la loi du 17 août 2018 relative à l'archivage) ;
- faire vérifier, par les services compétents, les équipements utilisés lors du déplacement en cas de doute sur leur intégrité.

A noter que l'agent reste tenu par ses obligations statutaires et légales, ainsi qu'à son obligation de confidentialité dans le cadre de déplacements professionnels.

Destruction de documents

L'agent doit garantir la confidentialité des données ainsi que des documents et informations professionnels non publics pendant tout leur cycle de vie.

De ce fait, leur destruction doit se faire de manière sécurisée, quel que soit leur support (électronique ou papier). Ainsi, il est interdit à l'agent de jeter des documents confidentiels ou contenant des données dans les poubelles ordinaires.

En revanche, l'agent doit détruire ces documents à l'aide de déchiqueteuses, à moins que des procédures mises en place par l'administration prévoient des procédures plus strictes (ex. : le recours à des poubelles sécurisées fournies par des prestataires certifiés procédant à une destruction irréversible).

Le service des imprimés et fournitures de bureau (« IFB ») du CTIE peut être mandaté par les administrations pour la destruction de leurs documents (mise à disposition de bacs pour l'enlèvement de documents obsolètes avec destructions des données confidentielles).

A noter que la destruction doit se faire dans le respect des dispositions de la loi du 17 août 2018 relative à l'archivage et des engagements pris par l'administration dans le tableau de tri cosigné avec les Archives nationales.

Mises à jour

Les équipements informatiques, les solutions techniques et les logiciels fournis par l'administration doivent être mis à jour **dans les meilleurs délais.**

Bien que les processus de mise à jour puissent être ressentis comme une contrainte, notamment lorsqu'ils interrompent une activité professionnelle, **l'agent ne doit pas retarder les mises à jour** ou ignorer les messages indiquant leur disponibilité.

Les services compétents pour la gestion de ces dispositifs (ex. : le CTIE), définissent les règles et processus de mises à jour. Elles sont ensuite portées à l'attention de l'agent.

Les vidéoconférences

Les outils de vidéoconférence font partie des outils indispensables à disposition des agents, en particulier dans le contexte du télétravail.

Le recours à ce type d'outil présente toutefois des risques en termes de sécurité de l'information. La mauvaise utilisation ou le paramétrage erroné des systèmes ainsi que l'existence de failles logicielles peuvent compromettre les données (ex. : écoute non autorisée de discussions, prise de contrôle de la caméra de participants). Par ailleurs, le partage de documents contenant des informations sensibles via une plateforme de vidéoconférence non gérée par les administrations publiques peut avoir pour conséquence que les informations transitent sur des serveurs non maîtrisés.

Afin de se prémunir contre ces conséquences dommageables, l'agent doit notamment :

- recourir à des plateformes de vidéoconférence gérées ou recommandées par les administrations publiques, telles que le CTIE ;
- s'assurer que seules les personnes habilitées participent à la vidéoconférence, notamment en restant attentif aux nouvelles connexions et à la liste des participants au cours de la réunion ;
- utiliser, si possible, la fonction « salle d'attente » pour filtrer les participants à la réunion, notamment lorsque la plateforme ne permet pas de restreindre l'accès par mot de passe ;
- ne pas enregistrer les vidéoconférences, à moins d'avoir préalablement recueilli le consentement des personnes concernées ou d'y être autorisé par ou en vertu de la loi ;
- éviter tout partage d'écran indésirable ;
- à la fin de la vidéoconférence, s'assurer de fermer la session en cours.

La loi du 11 août 1982 concernant la protection de la vie privée prévoit que toute atteinte volontaire à la vie privée d'autrui en écoutant ou en enregistrant, au moyen d'un appareil quelconque, des paroles prononcées en privé ou en observant une personne dans un lieu non accessible au public, sans le consentement de celle-ci, est sanctionnée pénalement.

La politique du bureau propre et de l'écran verrouillé (« Clean desk policy »)

Afin de réduire les risques d'accès non autorisé, de perte et d'endommagement d'informations confidentielles et de données, l'agent doit mettre en œuvre une politique de bureau propre et d'écran verrouillé, chaque fois qu'il s'absente de son poste de travail.

Dans ce contexte, il doit notamment :

- ranger son espace de travail lorsqu'il quitte son poste de travail ou lorsqu'il reçoit un visiteur dans son bureau et conserver les documents papiers de manière sécurisée (ex. : armoires de bureau fermées à clé) ;
- ne pas laisser sans supervision des documents confidentiels dans l'imprimante, la photocopieuse, ou sur le bureau ou tout autre endroit potentiellement exposé ;
- ne pas conserver des documents et des données dans des lieux accessibles à des personnes non autorisées ;
- mettre son ordinateur en mode veille, en cas d'absence prolongée, et l'éteindre en dehors des heures de bureau.

Besoin d'en connaître (« need to know »)

L'agent doit traiter les données dans les strictes limites des missions d'intérêt public poursuivies par l'administration et pour les seuls objectifs fixés par celle-ci dans le cadre de ses attributions.

Tout détournement et toute communication à des tiers contraires aux lois et règlements sont interdits.

La consultation à des fins privées de données contenues dans un fichier tenu par l'administration, tel que le registre national des personnes physiques (RNPP), constitue un détournement de finalité strictement interdit par la loi. Il en va de même pour les consultations à des fins privées, par les agents communaux, notamment du registre d'état civil.

L'agent ne doit pas transmettre ou divulguer des données à un destinataire (interne ou externe à l'administration) qui ne remplit pas, au moment de la réception des données, les conditions dans lesquelles il est habilité à les traiter.

En outre, il doit informer son supérieur hiérarchique dans les meilleurs délais lorsqu'il constate qu'il dispose d'accès indus (ex. : des droits qui n'auraient pas été supprimés après un changement d'affectation).

La sécurité des locaux de l'administration

L'agent doit respecter les mesures de sécurité physiques mises en place par l'administration et ne pas tenter de les contourner. Il ne doit, en particulier, pas :

- empêcher la fermeture d'une porte d'entrée contrôlée, que ce soit par courtoisie (ex. : tenir la porte ouverte à des personnes inconnues) ou par facilité (ex. : bloquer la porte d'entrée durant l'intervention d'un technicien) ;
- prêter son badge à autrui ;
- permettre à une personne d'accéder à une zone contrôlée sans que celle-ci ne se soit conformée aux procédures préalables de vérification existantes (ex. : protocole d'accueil des visiteurs) ;
- laisser un visiteur circuler sans surveillance dans les locaux de l'administration.

Au contraire, il doit contribuer à la sécurité des locaux de l'administration en restant vigilant et en signalant sans délai à ses supérieurs hiérarchiques toute suspicion de présence d'une personne non autorisée.

Les appels téléphoniques

L'agent doit veiller à ne pas divulguer des informations confidentielles à des personnes non habilitées ou malveillantes à travers le canal de communication des appels téléphoniques.

Pour ne pas communiquer de données à des personnes non autorisées, l'agent doit en particulier :

- vérifier l'identité de l'interlocuteur en lui demandant des informations précises (ex. : nom, prénom ainsi que matricule, couplés à des informations appropriées en fonction du contexte telles que le numéro de dossier) ;
- s'interroger sur la crédibilité d'une demande en tenant compte des éléments factuels ;
- vérifier, le cas échéant, les informations fournies par l'interlocuteur (ex. : en contactant l'organisation citée via des coordonnées publiques ou précédemment connues).

Le télétravail

Le télétravail permet à un agent de réaliser son activité professionnelle en dehors de son lieu de travail habituel.

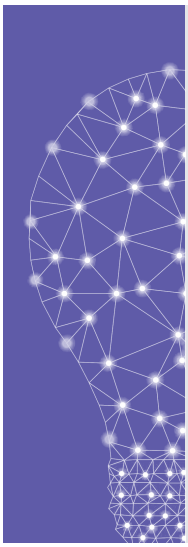
L'agent doit utiliser les équipements et accès professionnels de manière responsable et vigilante quand il travaille à distance. Ainsi, il est notamment tenu :

- d'appliquer rigoureusement les politiques et standards de sécurité mis en place par l'administration (ex. : respect de la Charte de bonne conduite en matière de sécurité de l'information numérique de l'ANSSI). Dans ce contexte, il reste soumis aux mêmes obligations que l'utilisateur travaillant sur site ;
- de s'abstenir de connecter ses équipements professionnels à des réseaux publics non maîtrisés ou non sécurisés ;
- de sécuriser le réseau domestique utilisé par un paramétrage approprié (ex. : routeur privé de connexion Internet sécurisé par mot de passe) ;
- d'utiliser le réseau VPN mis à disposition par l'administration ou le cas échéant par le gestionnaire informatique ;
- d'utiliser les équipements et outils informatiques de manière responsable (ex. : séparer les usages privés des usages professionnels) ;
- de rester vigilant quant aux tentatives d'attaques informatiques (ex. : attaque phishing, ingénierie sociale).

L'agent en télétravail est également tenu de prévoir un espace dédié à ses activités professionnelles qui garantit la confidentialité des informations qu'il traite. Pendant les heures de travail, cet espace ne doit pas être accessible à des tiers (ex. : membres de la famille). En effet, il convient de veiller à ce que les discussions professionnelles restent confidentielles, en particulier lors de l'utilisation d'outils de vidéoconférence à domicile, et de s'assurer à ce qu'aucun tiers n'accède aux informations que l'agent traite dans le cadre de l'exercice de ses fonctions.

« Clever clicks »

Un danger répandu de la sécurité de l'information consiste à inciter l'utilisateur à cliquer sur un lien suspect placé dans un mail (ex. : attaque phishing), à télécharger un logiciel malveillant (ex. : cheval de Troie) ou à utiliser des QR-Codes qui mènent à des sites corrompus. Pour s'en prémunir, **l'agent doit éviter de cliquer de manière imprudente sur des liens ou des applications** (« clever clicks »).



L'agent peut éviter de nombreux problèmes de sécurité de l'information en respectant notamment les bonnes pratiques suivantes :

- *ne télécharger de logiciels qu'à partir des sources vérifiées par l'administration publique, en particulier le CTIE ou le gestionnaire du réseau informatique ;*
- *en cas de doute par rapport à un lien contenu dans un mail, ne pas cliquer dessus sans avoir eu au préalable la confirmation par les organes compétents (ex. : le GOVCERT) de son caractère non nuisible ;*
- *ne pas « couper ou copier » un lien suspect se trouvant dans un mail ou SMS pour ensuite le « coller » dans son navigateur ;*
- *faire preuve de prudence face à tout type de pièce jointe dans un système de messagerie, même si elle provient d'un expéditeur connu ;*
- *se déconnecter correctement de son accès lorsque l'on quitte une application ;*
- *ne pas répondre à un message frauduleux, mais le signaler au service compétent.*

Ainsi, l'agent doit faire preuve d'une prudence accrue lors de la navigation sur Internet dans le cadre de ses activités professionnelles.

Contacter les services compétents en cas de questions ou de doutes

En cas de doutes, de suspicions d'une attaque ou d'un risque pour la sécurité de l'information, l'agent doit contacter son supérieur hiérarchique ainsi que les services de sécurité de l'information compétents de son administration (ex. : le gestionnaire informatique, tel que le CTIE, le GOVCERT, le RSSI, si désigné par l'administration, et le DPD).

CHAPITRE 3 //
LA SURVENANCE ET LA DÉTECTION DES INCIDENTS DE SÉCURITÉ ET DES VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL

SECTION 1 :
UN RISQUE OMNIPRÉSENT

L'objectif de la sécurité de l'information et des données est de réduire le risque de survenance d'un incident sur les actifs de l'administration et sur les informations et données qu'elle traite. Malgré toutes les mesures appropriées mises en œuvre, il ne saurait toutefois être exclu qu'une menace de la sécurité de l'information se concrétise et qu'une violation de données à caractère personnel se produise.

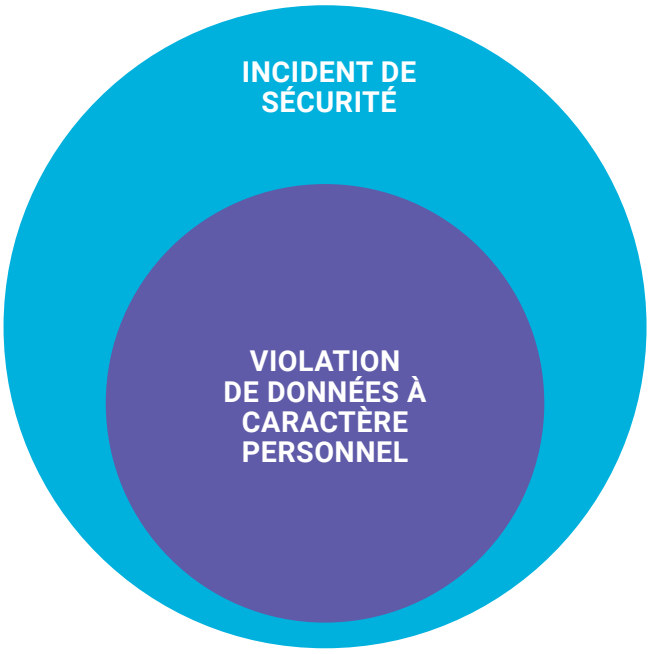
La notion d'« **incident de sécurité de l'information** » renvoie à tout évènement indésirable qui porte atteinte, en particulier, à la disponibilité, la confidentialité ou l'intégrité d'une information.

A noter qu'une indisponibilité planifiée des systèmes, notamment pour des raisons de maintenance, ne sera pas considérée comme un incident de sécurité.

La notion de « **violation de données à caractère personnel** » au sens du RGPD est plus restreinte que celle d'« incident de sécurité de l'information » en ce qu'elle ne vise que les situations dans lesquelles l'incident de sécurité porte sur des données à caractère personnel. Elle constitue ainsi un type particulier d'incident de sécurité.

A noter que les incidents de sécurité, tout comme les violations de données à caractère personnel, peuvent résulter d'un acte intentionnel, malveillant ou de nature accidentelle. Ils peuvent provenir d'une menace extérieure à l'administration ou relever d'un acte interne à celle-ci (ex. : violation de la politique de sécurité).

Les concepts d'« incident de sécurité de l'information » et de « violation de données à caractère personnel » au sens du RGPD sont donc des concepts différents, qui toutefois se superposent.



En d'autres termes, une violation de données au sens du RGPD constitue toujours un incident de sécurité de l'information. En revanche, un incident de sécurité de l'information n'est à qualifier de violation de données à caractère personnel au sens du RGPD que si des données à caractère personnel sont concernées.

SECTION 2 :
LES PRINCIPAUX TYPES D'ATTAQUES ET CAUSES D'INCIDENTS DE SÉCURITÉ

L'erreur humaine

L'erreur humaine figure parmi les principales causes d'incidents de sécurité. Il en existe un large éventail susceptible de porter atteinte à la sécurité des informations et des données, tel que l'envoi d'un mail au mauvais destinataire, la communication d'informations à des personnes sans vérification préalable de leur identité et habilitation ou l'oubli de documents confidentiels dans un lieu public ou non sécurisé.

D'après les statistiques de la CNPD pour l'année 2021, l'erreur humaine est la cause principale des violations de données à caractère personnel qui lui ont été notifiées (62%).

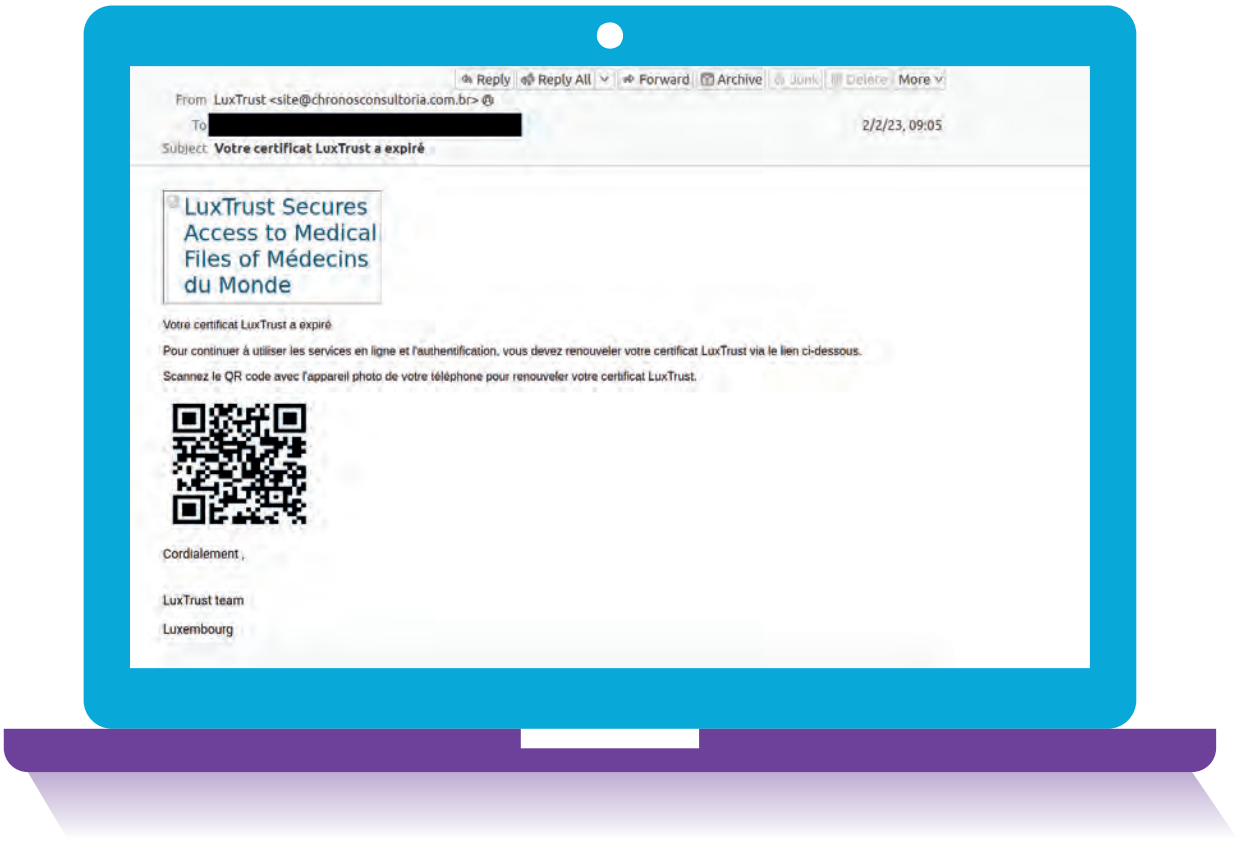
L'hameçonnage (« phishing »)

Le phishing est une forme d'escroquerie sur Internet employée par une personne malveillante pour récupérer des informations et des données traitées par un autre individu. L'attaquant se fait passer pour un organisme de confiance et incite ainsi la victime potentielle à l'ouverture d'une pièce-jointe malveillante, à l'accès à un site web contrefait ou à la communication de mots de passe ou d'informations confidentielles.

Pour ce faire, l'attaquant utilise le plus souvent le canal de la messagerie électronique en envoyant un mail reprenant la mise en page, le nom et le logo de l'entité dont il usurpe l'identité et en y intégrant la pièce jointe ou le lien frauduleux.

L'objectif de cette manœuvre est d'inciter l'agent, sous un faux prétexte, à se rendre sur un site web contrefait et à y introduire ses données (ex. : mise à jour d'un compte en ligne en cours d'expiration) ou à ouvrir une pièce jointe malveillante (ex. : contenant un virus).

Exemple d'un mail de « phishing » :

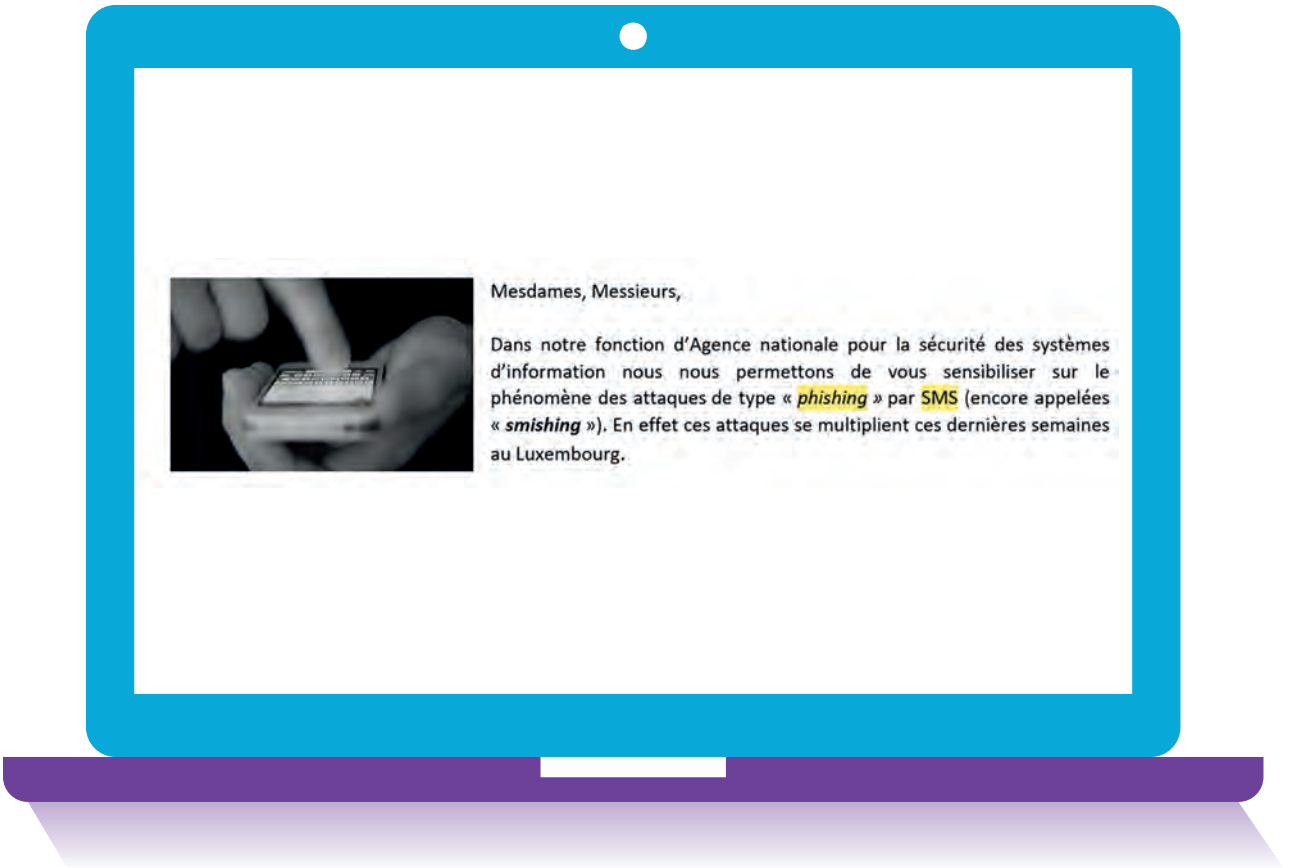


Bien que le but soit toujours le même, les attaques de phishing peuvent également prendre d'autres formes. Une méthode de phishing de plus en plus répandue consiste en l'envoi de SMS frauduleux renvoyant vers des sites Internet contrefaits.

Dans le cadre des campagnes de sensibilisation des agents étatiques, l'ANSSI rend attentif à l'existence d'attaques de type « phishing » par SMS (encore appelées « smishing ») s'appuyant sur la manipulation psychologique de la victime pour compromettre des systèmes d'information.

Très souvent, le message de « smishing » crée un sentiment d'urgence. Les messages peuvent contenir des mots ou phrases comme « action immédiate requise », « votre compte a été compromis » ou « vous vous exposez à des poursuites judiciaires si vous ne réagissez pas ».

Ces SMS frauduleux sont envoyés dans le but d'inciter le destinataire à ouvrir un lien transmis. L'utilisateur est ensuite invité à y saisir des informations personnelles, comme par exemple des coordonnées bancaires ou des données d'identification en ligne.



Les attaques de phishing peuvent avoir des **conséquences graves** pour la victime. Sur base des informations fournies par cette dernière, les attaquants vont pouvoir obtenir des avantages notamment :

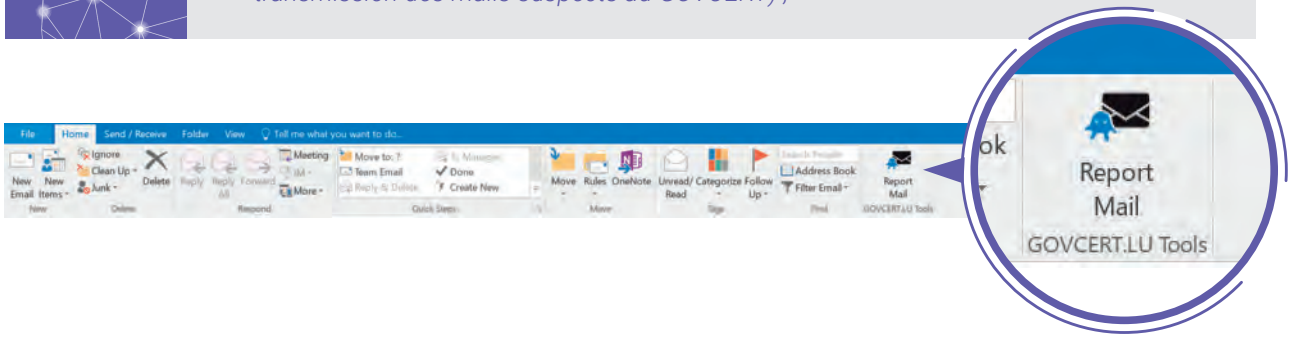
FINANCIERS (EX. : DÉTOURNEMENT D'ARGENT)

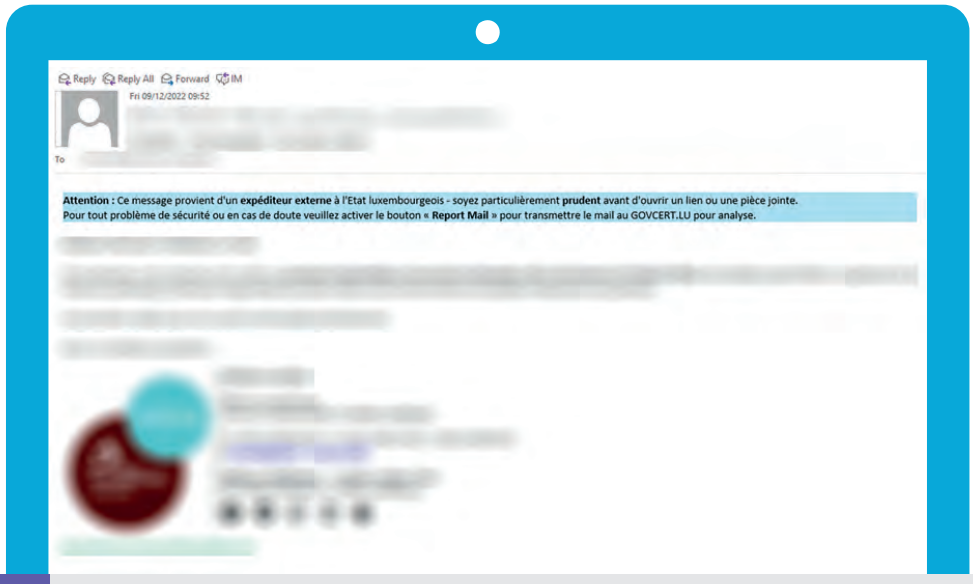
MATÉRIELS (EX. : ACCÈS AUX SYSTÈMES D'INFORMATION DE L'ADMINISTRATION)

MORAUX (EX. : EXERCICE DE PRESSION SUR LA VICTIME)

Les moyens de prévention :

- *transmettre immédiatement au GOVCERT les mails suspects. Pour ce faire, l'agent peut notamment utiliser la fonction « Report Mail » dans sa boite mail « Outlook ». Sur base de ce signalement, le GOVCERT informe l'agent du caractère malveillant ou non du mail (à noter que certaines entités ont prévu que leur RSSI soit le point de contact pour la transmission des mails suspects au GOVCERT) ;*





- *être particulièrement vigilant lorsque le message provient de l'extérieur (signalé par une bannière d'information du CTIE) ;*
- *contrôler si le message est personnellement adressé au destinataire ;*
- *vérifier la qualité rédactionnelle du message (ex. : fautes, traductions erronées, formules de politesse et de salutation inadaptées au contexte, signature du mail différente de la signature officielle, etc.) ;*
- *vérifier l'adresse d'expédition (ex. : annuaire public ou carnet d'adresses fiables), le cas échéant, en contactant l'expéditeur par un canal officiel et fiable pour s'assurer qu'il est bien à l'origine du message ;*
- *vérifier l'authenticité de l'adresse web (URL) du navigateur avant de s'authentifier.*

*Par ailleurs, il convient d'**être d'autant plus vigilant face à un mail qui porte sur une demande de communication d'informations personnelles** ou qui comporte des pièces jointes ou des liens externes.*

Le « spear phishing »

Les attaques de spear phishing sont une forme particulière de phishing qui s'appuient généralement sur des tactiques poussées d'ingénierie sociale.

Elles consistent, tout comme les attaques de phishing classiques, dans l'usurpation de l'identité numérique d'un tiers et visent à duper le destinataire en vue de l'inciter à ouvrir une pièce jointe ou un lien vers un site Internet malveillant. Toutefois, s'y ajoute un élément frauduleux supplémentaire, à savoir un ciblage très précis qui s'adresse au destinataire du message.

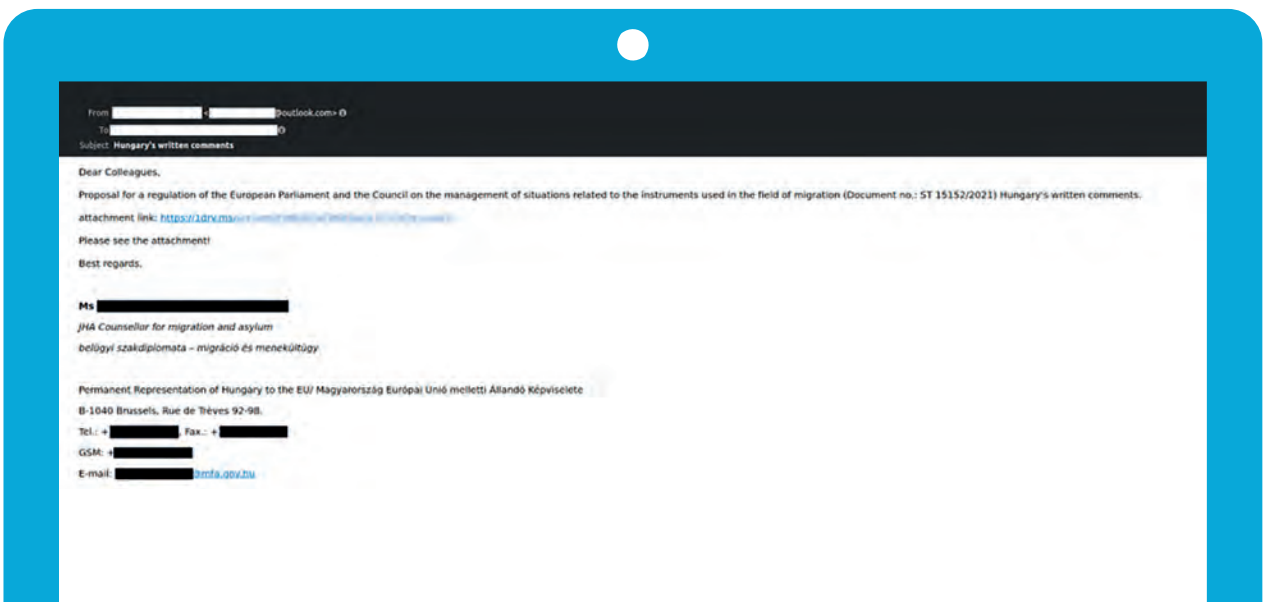
Ainsi, les attaques de type spear phishing sont plus élaborées, hautement personnalisées et minutieusement préparées avant leurs mises en œuvre.

Les moyens de prévention :

Quelques éléments suspects permettent d'identifier qu'il s'agit d'une attaque de spear phishing, notamment :

- *les attaques de spear phishing se caractérisent par l'usage d'un compte mail spécifiquement créé, typiquement sur une plateforme de messagerie publique (Outlook, Gmail, etc.), pour usurper l'identité d'un tiers (ex. : le mail est envoyé à partir d'une adresse Outlook sous la forme : firstname. lastname@outlook.com avec « first name » et « last name » étant le prénom et nom d'un agent usurpé) ;*
- *l'objet du mail est souvent lié à un sujet d'intérêt actuel pour susciter l'attention de la victime ciblée et l'inciter à l'ouvrir ;*
- *contrairement aux mails de type phishing, ceux de type spear phishing sont, en principe, mieux rédigés (pas ou peu de fautes de grammaire, brève explication sur le sujet, renvoi à un document contenant des informations supplémentaires, etc.) ;*
- *le lien (« hyperlink ») ajouté au mail de spear phishing peut être modifié quant à son apparence grâce à la fonctionnalité « modifier le lien hypertexte ». Ceci permet à l'attaquant d'induire sa victime en erreur en la dirigeant sur un site Internet malveillant paraissant tout à fait légitime (une lettre ou un caractère en trop ou en moins peut conduire vers un tout autre site web). Pour éviter des renvois frauduleux, une option est de privilégier la saisie des URL directement dans la barre d'adresses.*

Exemple d'un mail de « spear phishing » :


From [redacted]outlook.com>
To [redacted]
Subject: Hungary's written comments

Dear Colleagues,

Proposal for a regulation of the European Parliament and the Council on the management of situations related to the instruments used in the field of migration (Document no.: ST 15152/2021) Hungary's written comments.

attachment link: https://1drv.ms/[redacted]

Please see the attachment!

Best regards,

Ms [redacted]
JHA Counsellor for migration and asylum
belügyi szakdiplomata – migráció és menekültügy

Permanent Representation of Hungary to the EU/ Magyarország Európai Unió melletti Állandó Képviselete
B-1040 Brussels, Rue de Trèves 92-98.
Tel.: +[redacted], Fax.: +[redacted]
GSM: +[redacted]
E-mail: [redacted]@mfa.gov.hu

Illustration - site Internet original :

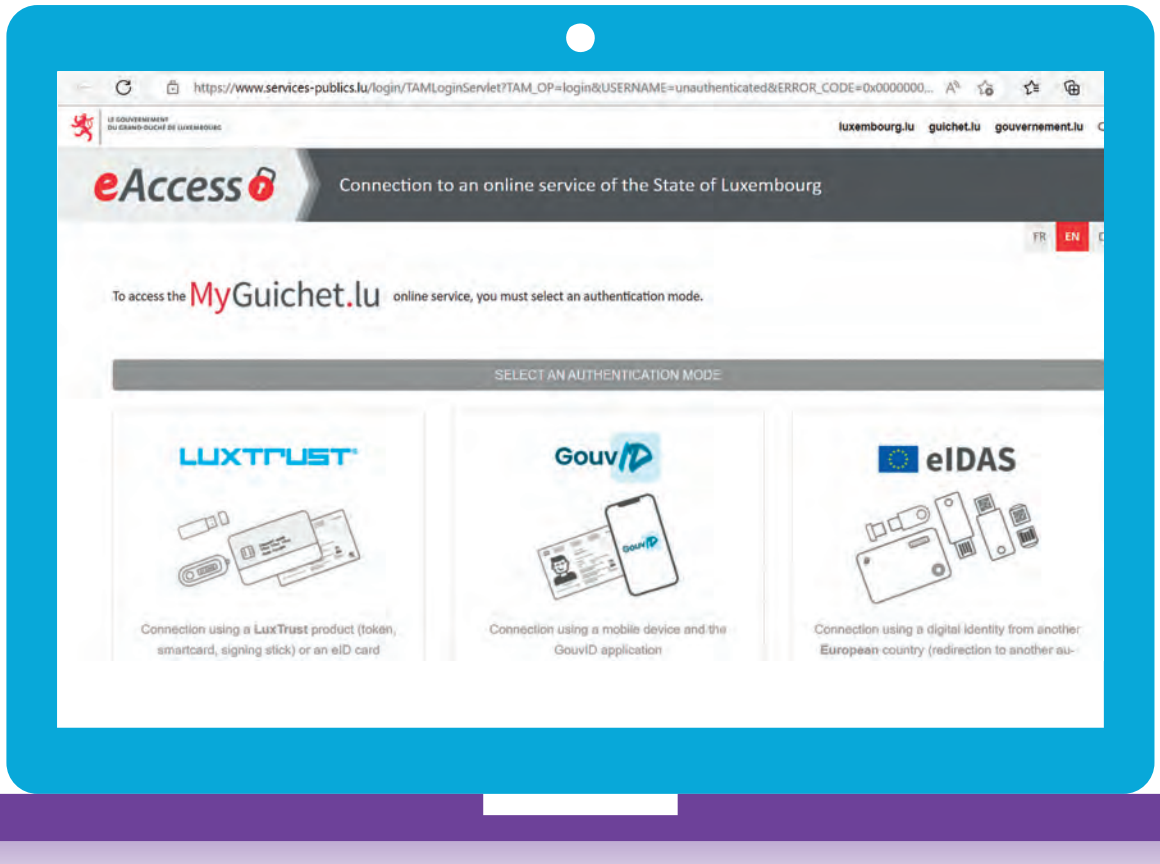
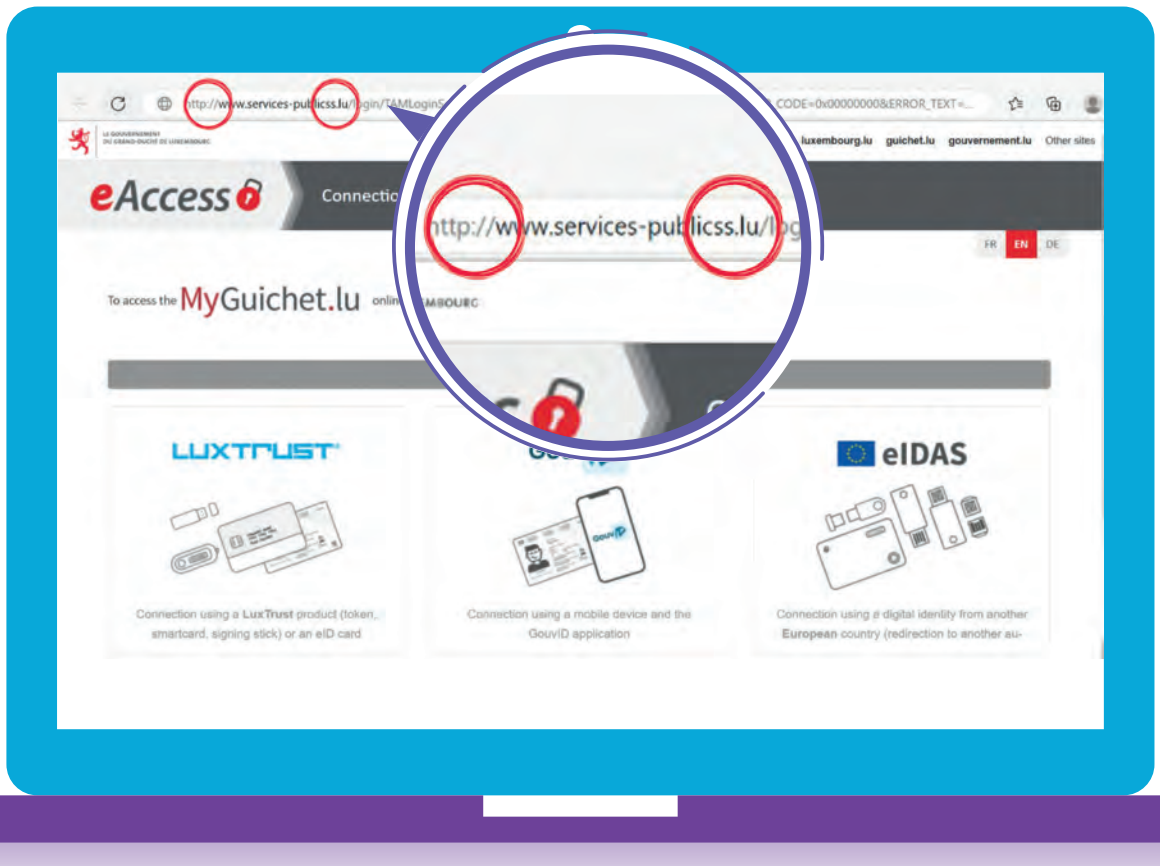


Illustration - site Internet corrompu :



L'ingénierie sociale (« social engineering »)

L'ingénierie sociale est une technique de manipulation humaine qui consiste à obtenir de la victime un bien ou une information à laquelle celle-ci peut accéder, directement ou indirectement, en exploitant sa confiance, son ignorance ou sa naïveté. Le facteur humain est le point central de ce type d'attaque.

L'attaque d'ingénierie sociale peut survenir dans la vie de tous les jours ainsi que sur le lieu de travail. Pour extorquer des informations ou des biens, il n'est pas rare que l'attaquant étudie au préalable les environnements personnel et professionnel de sa future victime afin d'établir, dans une première phase, une relation de confiance avec cette dernière.

Souvent les attaquants se dotent d'une connaissance approfondie du jargon employé par l'administration et des procédures mises en place par celle-ci. Cette manière de procéder facilite la prise de contact et permet de rendre la demande de l'attaquant crédible.

Les rapports entre l'attaquant et la victime peuvent prendre différentes formes. Elles peuvent notamment se faire via :

TÉLÉPHONE | **RÉSEAUX SOCIAUX** | **MAIL** | **PRÉSENCE PHYSIQUE DE L'ATTAQUANT**

Les moyens de prévention :

- *prendre le temps de réfléchir et éviter les décisions impulsives sous la pression de l'attaquant (ex. : ne pas divulguer ses identifiants ni son mot de passe, même si la demande semble crédible) ;*
- *ne pas révéler d'informations confidentielles sur les réseaux sociaux ;*
- *ne pas répondre à des demandes d'informations, voire à des instructions illicites ou émanant de sources non vérifiées ;*
- *rester vigilant dès qu'une personne inconnue adopte un comportement trop curieux, en particulier en ce qui concerne les activités professionnelles de l'agent.*

La fraude au président

La fraude au président consiste en l'usurpation de l'identité d'un membre de la direction de l'administration.

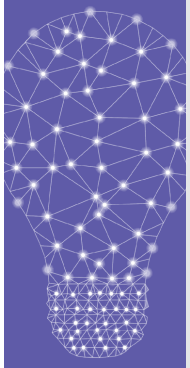
L'objectif de cette attaque est de convaincre l'agent que la demande ou l'ordre émane de sa hiérarchie et de l'inciter ainsi à effectuer une démarche bénéfique à l'attaquant, telle qu'un transfert d'argent sur un compte bancaire.

La plupart du temps, une fraude au président se déroule en **3 étapes** :

1. L'attaquant analyse l'environnement de l'administration et collecte toutes sortes d'informations disponibles (ex. : annuaire, organigramme, rapports annuels).
2. L'attaquant se fait passer auprès de l'agent pour un membre de sa hiérarchie dont il a usurpé l'identité.
3. L'attaquant utilise l'identité usurpée pour inciter l'agent à effectuer une démarche à son bénéfice, que ce soit par des moyens élaborés (ex. : mail contrefait en combinaison avec des techniques d'ingénierie sociale) ou non (ex. : appel téléphonique avec un numéro masqué).

Cela étant dit, il existe également d'autres formes de ce type d'attaque par usurpation d'identité dans lesquelles l'auteur malveillant se fait passer pour un agent de l'administration (et non pas pour un membre de la direction), par exemple, pour demander au service des ressources humaines un changement de compte bancaire pour le virement de sa rémunération.

L'essor des nouvelles technologies, en particulier les avancées liées à l'intelligence artificielle, permet aux personnes malveillantes de disposer d'outils numériques accroissant la crédibilité de leur attaque. Parmi ces techniques figure notamment celle de la « Deepfake voice » consistant en la création d'une voix de synthèse imitant la voix d'une personne à partir d'enregistrements sonores et vidéos collectés par l'attaquant.



Les moyens de prévention :

- *respecter les procédures de vérifications et de signatures multiples, en particulier pour les transactions bancaires ;*
- *porter un regard critique sur les demandes ou instructions inhabituelles ;*
- *accentuer la vigilance lors des périodes de congés scolaires, jours fériés ainsi que de manière générale en dehors des heures de bureau ;*
- *contacter immédiatement la hiérarchie avec les coordonnées officielles (ex. : annuaire de l'Etat) en cas de doute et s'abstenir d'exécuter définitivement les démarches sollicitées sans confirmation complémentaire ;*
- *ne pas céder à la pression de l'attaquant.*

Le rançongiciel (« ransomware »)

Le ransomware est un type de cyberattaque qui consiste en l'introduction d'un programme malveillant dans les systèmes informatiques de la victime qui chiffre les informations y contenues. La plupart du temps, le ransomware est lancé par une action de l'utilisateur et plus rarement par une vulnérabilité technique permettant son entrée dans le réseau interne.

Le but de cette attaque est de rendre impossible la consultation et l'utilisation des informations par la victime. Ceci permet à l'attaquant d'extorquer à cette dernière le paiement d'une rançon en contrepartie de la clé de déchiffrement, voire de la garantie qu'il ne va pas vendre ou publier les informations en question.

A noter que l'Agence de l'Union européenne pour la cybersécurité (« ENISA ») a rapporté une augmentation de **234 %** *du nombre d'attaques par ransomware en 2021. En raison de cette évolution significative, l'ANSSI a élaboré des recommandations en la matière.*

Les moyens de prévention :

- *rester prudent lors de l'ouverture de mails, pièces-jointes ou liens suspects ;*
- *mettre à jour régulièrement les systèmes informatiques et applications ;*
- *ne pas installer de logiciels sans l'autorisation de l'administration ;*
- *en cas de suspicion de corruption de systèmes ou fichiers, contacter sans délai l'instance gestionnaire des incidents de sécurité interne désignée par l'administration et, en particulier, le GOVCERT ;*
- *en cas de suspicion de corruption de systèmes ou fichiers, débrancher la machine touchée par l'attaque du réseau d'Internet en vue d'éviter la propagation du programme malveillant dans les systèmes informatiques de l'administration ;*
- *ne pas éteindre la machine infectée (sans préjudice de l'obligation de débrancher la machine d'Internet) afin d'éviter toute perte de preuves et de traces liées à l'incident de sécurité.*

Le logiciel malicieux (« malware »)

Le malware est un programme développé pour nuire à un système informatique ou un réseau.

Il en existe plusieurs types, notamment :

- **le virus** est un logiciel qui accomplit une tâche malicieuse sur la machine de la victime, telle que le vol ou la modification des données. Il est transmis à la victime la plupart du temps au moyen d'une pièce jointe à un mail ou d'un « hardware » corrompu (ex. : une clé USB). Une fois activé (a priori suite à une action de l'utilisateur), il se transmet à tout équipement connecté à la machine infectée.

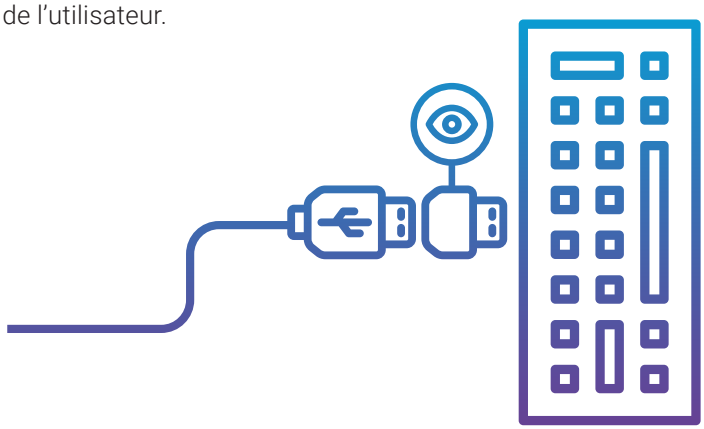
- **le ver** (« worm ») est une sous-catégorie de virus qui se propage de manière quasi autonome, principalement par le réseau, sans nécessiter une intervention humaine directe et ce, pour reproduire son code sur le plus grand nombre de machines possible. Une fois exécuté à l'insu de l'agent, il perturbe les systèmes concernés.

- **le « cheval de Troie »** est un type de logiciel malveillant qui prend souvent l'apparence d'un logiciel authentique. Il peut être utilisé par l'attaquant pour accéder aux systèmes et réseaux de la victime afin de pouvoir y exécuter des actions malveillantes à l'insu de celle-ci. Contrairement au virus et au ver, qui visent une propagation à grande échelle, le « cheval de Troie » ne recherche pas à s'auto-propager et à se diffuser sur des machines d'autres utilisateurs (notamment pour éviter la détection par des anti-virus). L'objectif du « cheval de Troie » est, en revanche, de rester inaperçu et de permettre à la personne malveillante de conduire des attaques plus ciblées sur ses victimes à partir de l'appareil infecté.

L'enregistreur de frappe (« keylogger »)

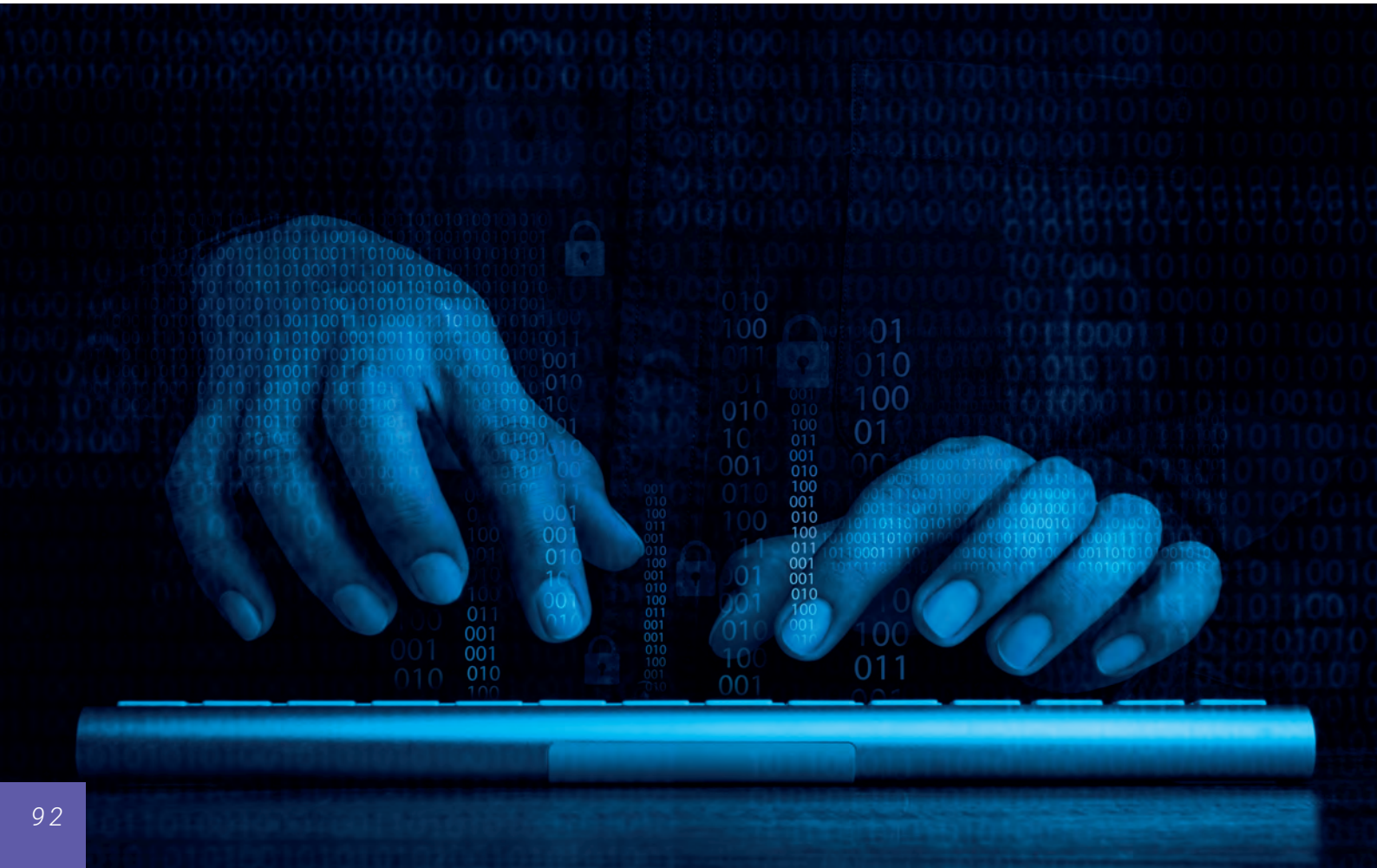
Le keylogger est un logiciel ou matériel malveillant déployé par un attaquant pour enregistrer et analyser les saisies effectuées par l'utilisateur sur le clavier de sa machine. Ce type d'attaque permet d'obtenir des informations en temps réel, à l'insu de l'agent, telles que son identifiant et son mot de passe.

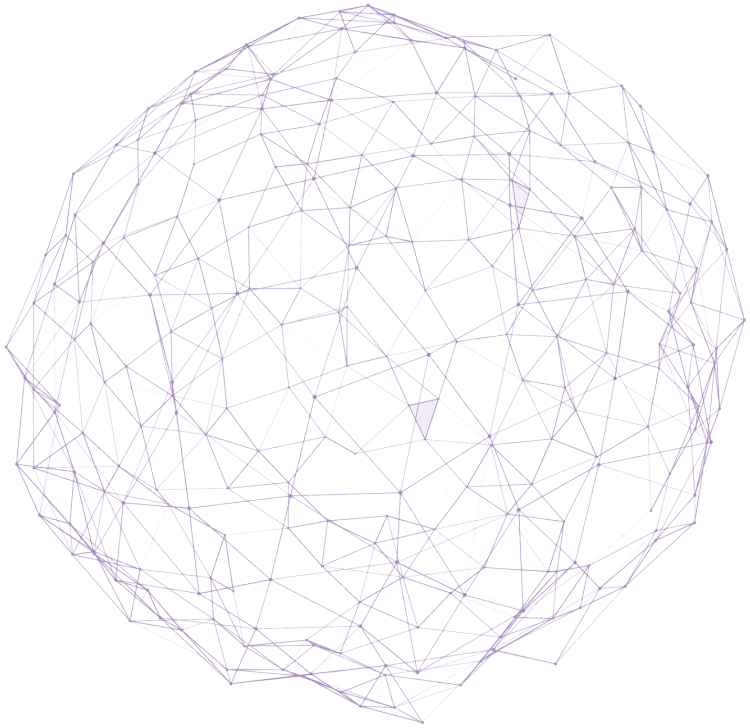
Les **keyloggers matériels** sont des dispositifs intercalés physiquement entre le clavier et la machine de l'utilisateur.



De ce fait, il convient notamment d'être vigilant face au matériel dont la provenance est susceptible d'engendrer un danger de sécurité (ex. : clé USB offerte lors d'un évènement).

Contrairement aux keyloggers matériels, les **keyloggers logiciels** ne sont pas visibles à l'œil nu. Il s'agit de logiciels d'espionnage qui sont programmés de manière à rester indétectables et à se lancer au cours du démarrage du système d'exploitation (ex. : démarrage du système Windows).

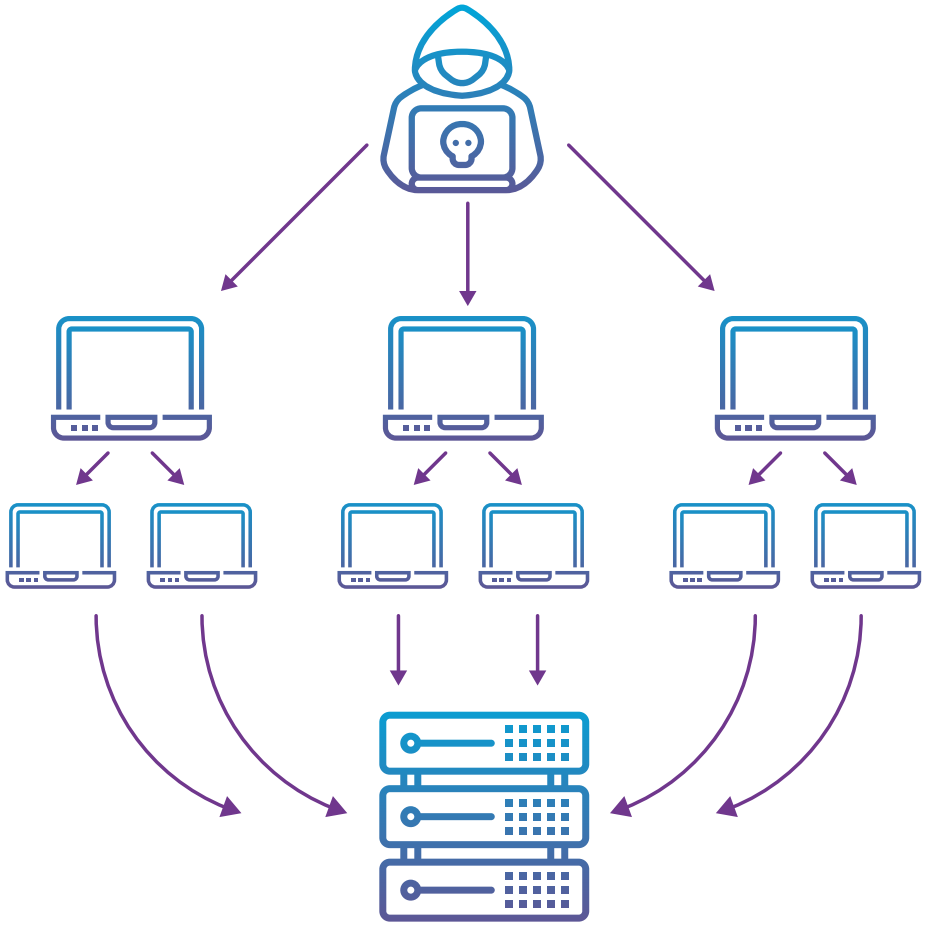




Le déni de service (« denial of service »)

L'objectif d'une attaque du type déni de service est de rendre inaccessible le serveur cible.

Pour ce faire, l'attaquant va, soit saturer le serveur en l'inondant de requêtes, soit provoquer un dysfonctionnement de celui-ci en exploitant une faille de sécurité. L'attaquant va téléguider des milliers de machines, infectées par un cheval de Troie, faisant partie d'un réseau dit « BOTNET » pour saturer un serveur par des millions de requêtes.



SECTION 3 :
L'OBLIGATION DE DÉTECTER LES INCIDENTS DE SÉCURITÉ ET LES VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL

La capacité de détecter et de gérer les incidents de sécurité, y compris les violations de données à caractère personnel, constitue un élément essentiel de la gestion de la sécurité de l'information et des données.

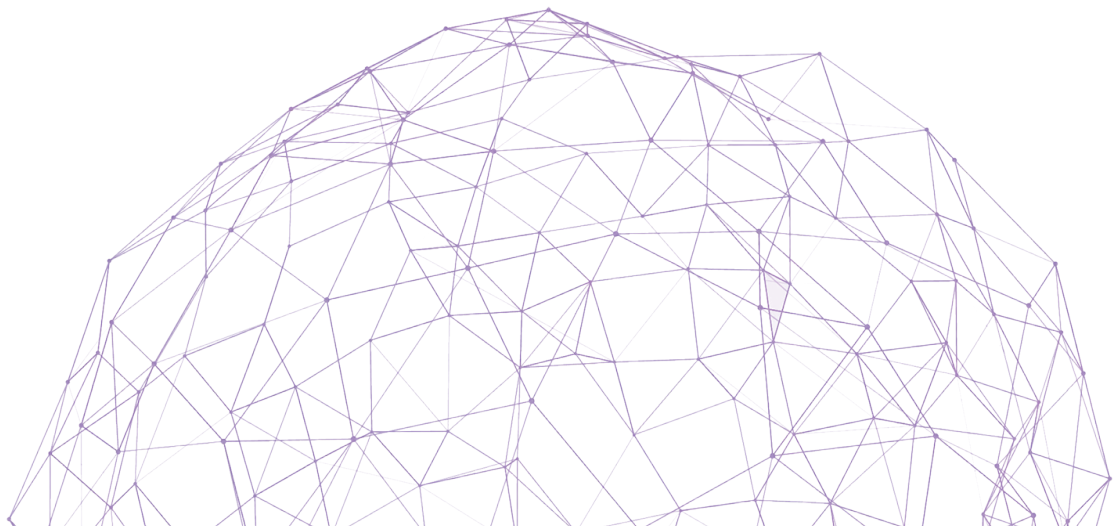
L'administration doit être en mesure de **réagir dans les meilleurs délais à un incident de sécurité et de le gérer de manière appropriée**, notamment en minimisant les conséquences néfastes tant sur les activités de l'administration que sur les droits et libertés des individus.

Elle doit pouvoir assurer une reprise des activités aussi rapide que possible et entreprendre les démarches de notification prévues par la loi dans les délais impartis.

Un élément important de la bonne gestion des incidents de sécurité et des violations de données au sens du RGPD est la **mise en œuvre de procédures internes** par l'administration (sans préjudice des autres mesures techniques et organisationnelles).

Ces procédures doivent notamment :

- informer les agents de leur obligation de signaler tout soupçon d'un incident de sécurité sans délai à l'instance gestionnaire des incidents de sécurité de l'information désignée par l'administration ;
- déterminer à qui les agents doivent signaler les incidents de sécurité en interne ;
- préciser comment les agents doivent rapporter les incidents de sécurité en interne ;
- préciser à qui revient la responsabilité opérationnelle au sein de l'administration de gérer les incidents de sécurité et les violations de données à caractère personnel.



SECTION 4 :
LE RÔLE DE L'AGENT DANS LA DÉTECTION DES INCIDENTS DE SÉCURITÉ

Le rôle central de l'agent dans la détection et la remontée des incidents de sécurité

L'agent a un rôle important à jouer afin de permettre à son administration de détecter les incidents de sécurité et les violations de données et de les gérer de manière appropriée.

L'agent doit :

- **informer, sans délai, l'instance gestionnaire des incidents de sécurité de l'information désignée par l'administration de tout soupçon d'incident de sécurité**, qu'il s'agisse ou non d'une violation de données ;
- **rapporter les faits qu'il a observés ainsi que les actions qu'il a entreprises**, en particulier juste avant et au cours de l'incident de sécurité, avec le plus de précision possible.

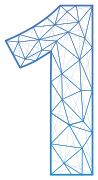
L'objectif de cette documentation et de cette remontée d'informations par l'agent est de permettre à l'administration de parvenir à une compréhension détaillée de l'incident.

Les bonnes pratiques à respecter par l'agent en cas de soupçon d'un incident de sécurité

L'agent doit mettre en œuvre les bonnes pratiques en cas de soupçon d'un incident de sécurité. Ainsi, il doit notamment :

Remonter des informations dans les meilleurs délais au niveau approprié

Le premier réflexe de l'agent doit être de contacter l'instance gestionnaire des incidents de sécurité de l'information désignée par son administration, dès qu'il a des raisons de soupçonner qu'un incident de sécurité (qu'il s'agisse ou non d'une violation de données) se produit ou est susceptible de se produire.



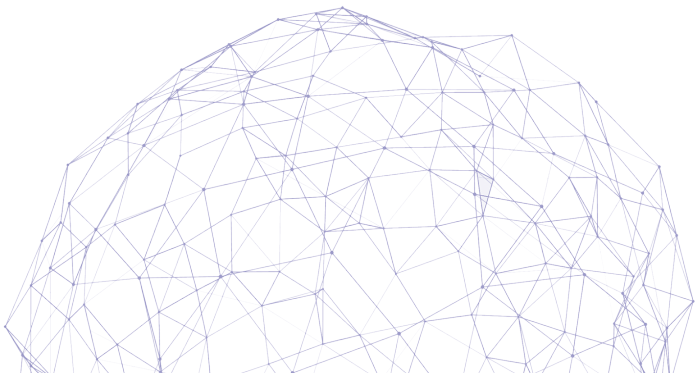
En pratique, il s'agit le plus souvent du :

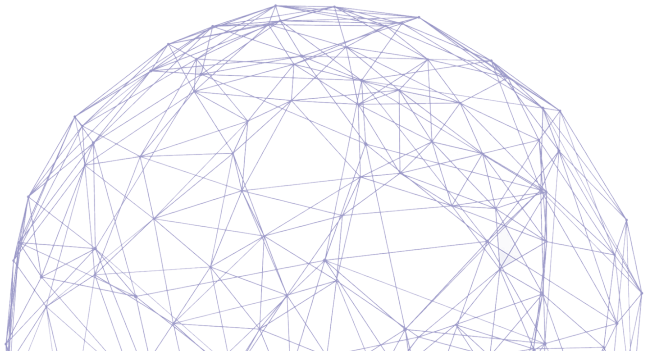
- *supérieur hiérarchique,*
- *support informatique de l'administration,*
- *RSSI, si désigné par l'administration, CTIE et GOVCERT,*
- *DPD.*

La réactivité de l'agent est essentielle. En effet, plus vite un incident sera signalé, plus les chances sont grandes d'en limiter les conséquences néfastes pour l'administration et pour les personnes concernées.

Ne pas dissimuler ou minimiser l'incident

L'agent doit signaler tout incident de sécurité potentiel avec le maximum de détails possible. Il ne doit pas omettre de faits liés à l'incident de sécurité ou en diminuer leur gravité, notamment en raison d'un sentiment de honte lié à son erreur, par crainte des conséquences éventuelles de ses actes (souvent l'agent étant lui-même victime), voire pour réduire son implication potentielle dans la production de l'incident (ex. : mauvaise manipulation).





Ne pas effectuer de qualification juridique de l'incident de sécurité

A moins que ce rôle ait expressément été attribué à l'agent par sa hiérarchie, il n'est pas de sa compétence de faire une analyse juridique et technique de la situation, voire une qualification juridique des faits (ex. : s'agit-il ou non d'une violation de données à caractère personnel au sens du RGPD ?).

Le rôle de l'agent consiste principalement à remonter des informations nécessaires au niveau approprié afin d'informer les services compétents de la survenance d'un incident potentiel. Il revient ensuite à ces services (ex. : le DPD, le RSSI, le CTIE, le GOVCERT) d'évaluer les démarches à entreprendre et de déterminer si un incident de sécurité de l'information est à qualifier de violation de données au sens du RGPD.

Ne pas essayer de résoudre seul le problème

En cas de soupçon d'un incident de sécurité, **l'agent doit s'abstenir de toute tentative de résoudre le problème de sa propre initiative**. Il doit agir sur base des procédures internes en vigueur ou sur base des instructions communiquées par l'instance gestionnaire des incidents de sécurité de l'information et informer les personnes en charge des violations de données.

Ne pas divulguer des informations confidentielles

L'obligation de confidentialité de l'agent ne s'éteint pas avec la survenance potentielle d'un incident de sécurité.

De ce fait, **l'agent doit rester vigilant et ne pas divulguer des informations relatives à l'incident à des personnes non autorisées**, tant pendant qu'après la survenance de l'incident.

Déconnecter la connexion Internet en cas de soupçon d'une cyberattaque

En cas d'un soupçon d'une cyberattaque, **l'agent doit immédiatement déconnecter sa machine du réseau Internet**, avec fil (par câble « Ethernet ») ou sans fil (ex. : Wifi, Bluetooth). Il doit également déconnecter toutes les machines qui seraient reliées à la sienne ou branchées sur le même réseau.

Le fait de déconnecter la machine évite la propagation de malwares, tels que les virus, dans les systèmes informatiques de l'administration.

Si l'agent constate un dysfonctionnement de sa machine (ex. : lenteur de réaction, ouverture de fichiers erronés, cryptage des informations en direct), il est possible, voire probable, qu'une attaque du type ransomware soit en train de se produire.

Dans pareil cas de figure, l'agent doit immédiatement déconnecter toutes les machines de son poste de travail susceptibles d'être infectées afin de confiner le malware. Par contre, comme évoqué ci-dessous, il ne doit jamais les éteindre pour éviter toute perte de preuves et de traces.

7

Ne pas débrancher la machine du réseau d'électricité, ni l'éteindre en cas de soupçon d'une cyberattaque

L'agent ne doit **pas retirer la prise électrique de sa machine, ni l'éteindre** en cas de soupçon d'une cyberattaque (sans préjudice de l'obligation de déconnecter la machine d'Internet) afin d'éviter toute perte de preuves liées à l'incident de sécurité.

Une partie des preuves liées aux attaques malveillantes sont sauvegardées sur la « mémoire vive » (la « RAM ») de chaque machine, c'est-à-dire sur la mémoire à court terme de la machine, où sont stockées les données actuellement utilisées par le processeur.

Compte tenu du fait que cette mémoire vive est effacée à chaque fois que la machine est éteinte ou redémarrée, l'agent doit s'abstenir d'entreprendre une telle démarche et veiller à ce que la machine ne s'éteigne pas ou ne redémarre pas à cause d'un acte externe (ex. : perte de batterie ou coupure d'électricité).

Sécuriser les preuves

Afin de faciliter le travail des experts en « data forensics », l'agent doit **documenter les faits, les actions entreprises ou observées ainsi que les évènements liés à l'incident de sécurité.**

La « data forensics » est une branche des sciences criminalistiques qui porte sur la recherche, l'acquisition, le traitement et l'analyse de données stockées sous forme numérique et sur la communication d'informations les concernant.

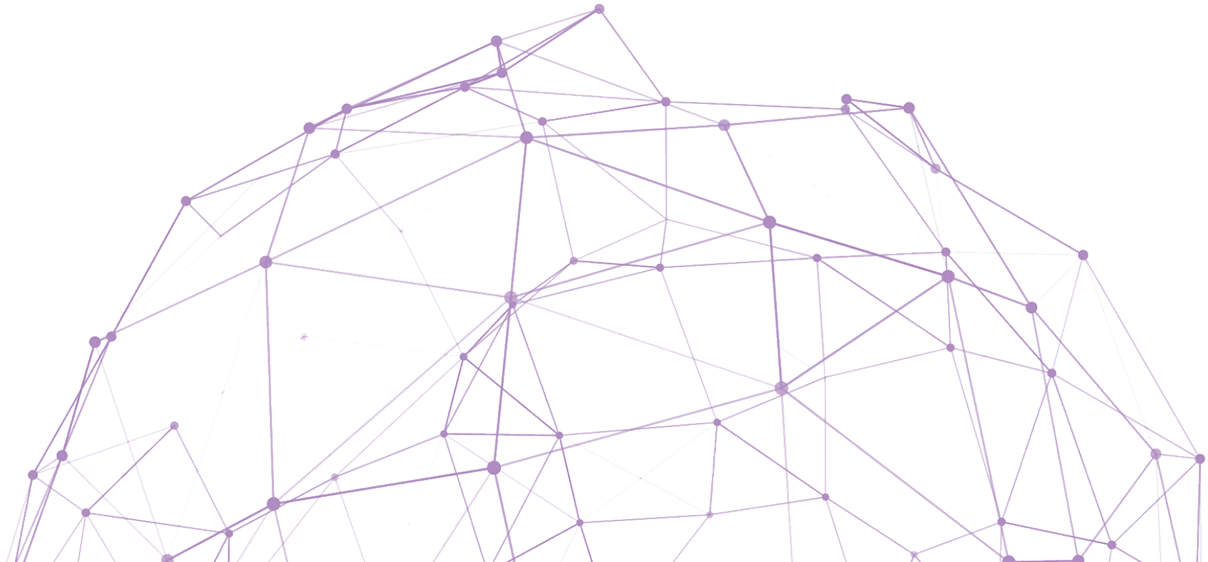
La documentation doit *a minima* comprendre :

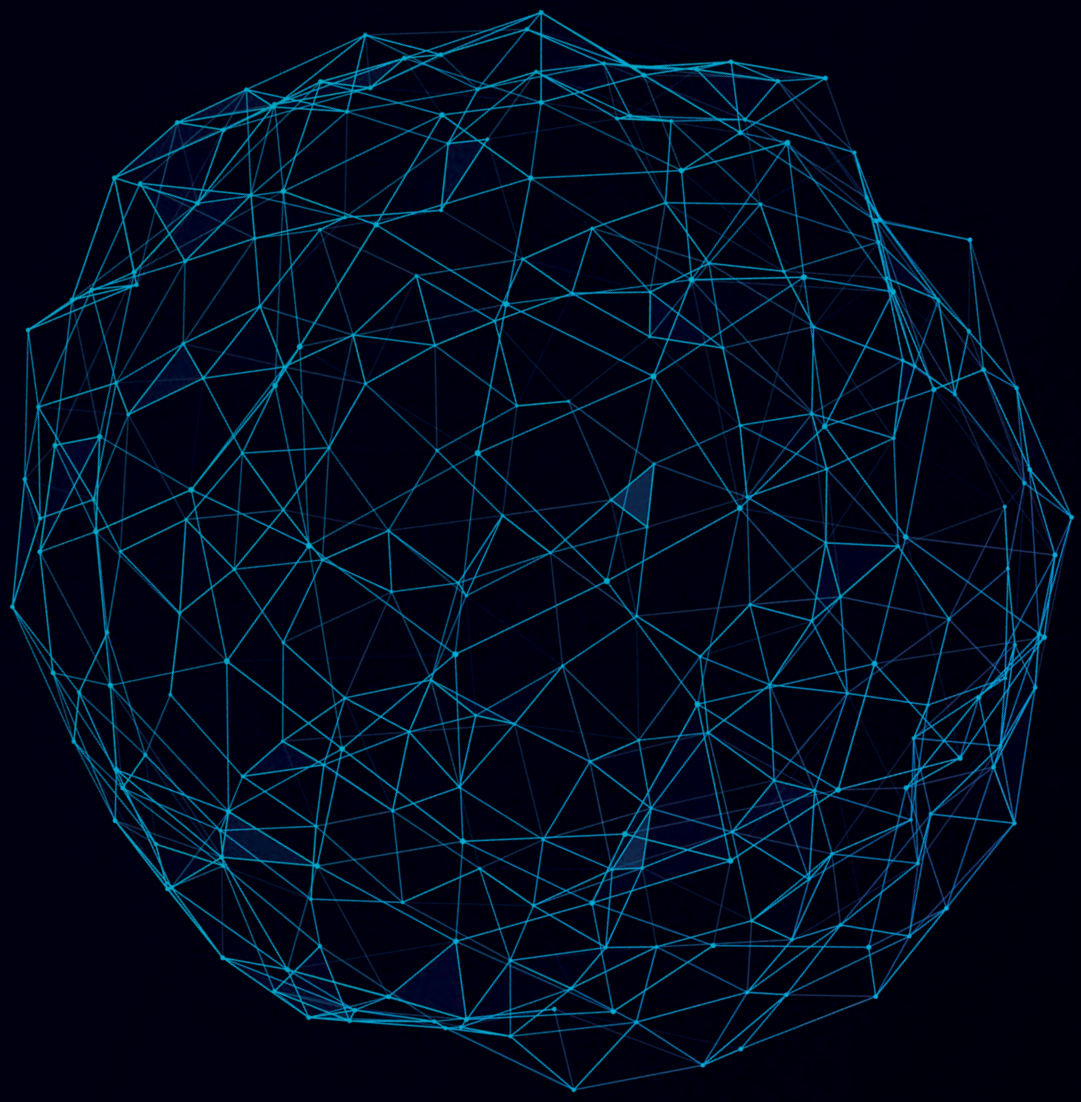
- l'identité des personnes impliquées dans le déroulement et la gestion de l'incident de sécurité ;
- une description chronologique détaillée de chaque action entreprise ou observée ainsi que des faits et évènements constatés (avec les dates et heures).

Dans une optique de documentation de l'incident de sécurité, des vidéos ou des photos de toute activité suspecte peuvent être prises par l'agent. Cette démarche sera utile aux experts en la matière pour contextualiser et comprendre l'incident de sécurité.

Changer le mot de passe en cas de compromission (réelle ou suspectée)

Dans l'hypothèse où une **compromission du mot de passe** est suspectée, **l'agent doit le modifier** dans les plus brefs délais afin de prévenir toute utilisation illicite par des tiers (sans préjudice de l'obligation de désactiver le compte en cas de doute).





CHAPITRE 4 //
LA GESTION DES « VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL » PAR L'ADMINISTRATION CONFORMÉMENT AU RGPD

SECTION 1 :
LE CONCEPT DE « VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL »

Le RGPD définit la « violation de données à caractère personnel » comme une « violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ».

On parle dès lors d'une violation de données au sens du RGPD, lorsqu'un incident de sécurité concerne des données à caractère personnel et entraîne, de manière accidentelle ou illicite :

LA DESTRUCTION DE DONNÉES

LA PERTE DE DONNÉES

L'ALTÉRATION DE DONNÉES

LA DIVULGATION NON AUTORISÉE DE DONNÉES TRANSMISES, CONSERVÉES OU TRAITÉES D'UNE AUTRE MANIÈRE

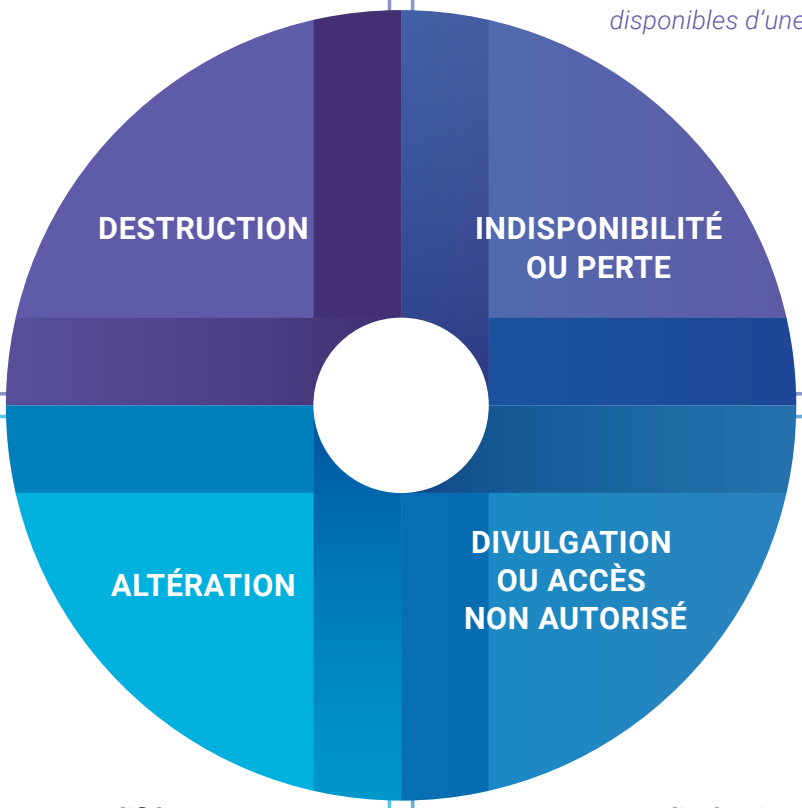
L'ACCÈS NON AUTORISÉ À DES DONNÉES

Les données n'existent plus sous une forme utile pour l'administration.

Exemple :
Destruction d'un original papier contenu dans un dossier d'un administré sans qu'il n'existe une copie électronique ou papier.

L'administration a perdu, de manière temporaire ou définitive, tout contrôle, possession ou accès aux données.

Exemple :
Les systèmes informatiques sur lesquels l'administration conserve les données ne sont pas accessibles et les données ne sont pas disponibles d'une autre manière.



Les données sont modifiées, corrompues, ou incomplètes.

Exemple :
En raison d'une mauvaise manipulation, la structure d'un fichier est modifiée de sorte que les données ne sont plus en lien avec la personne concernée.

Une divulgation non autorisée de données à autrui, ou un accès non autorisé aux bases de données de l'administration.

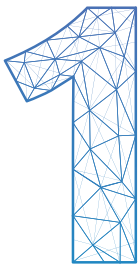
Exemple :
Envoi d'un courriel avec des données au mauvais destinataire (interne ou externe).

Les violations de données ne sont donc pas qualifiées en fonction d'un support (ex. : papier, clés USB, système informatique) ou d'un élément déclencheur (ex. : vol d'un document papier, incident de cybersécurité).

Tout comme un incident de la sécurité de l'information, une violation de données peut résulter d'un acte malveillant ou accidentel.

LES DIFFÉRENTS TYPES DE VIOLATIONS DE DONNÉES

Il existe **3 types de violations** de données, à savoir :



les **violations de confidentialité** : il s'agit des cas de divulgation ou d'accès non autorisé ou accidentel à des données.

Exemples :

- *envoi d'un mail contenant des données à un destinataire non-autorisé ;*
- *perte d'une clé USB sur laquelle sont enregistrées des données ;*
- *mauvaise configuration d'envoi de courriels en masse sans masquer les adresses des destinataires, qui sont alors visibles par tous les destinataires ;*
- *mauvais paramétrage qui ne procède pas à l'isolement d'un serveur sur lequel sont enregistrées des données le rendant ainsi librement accessible depuis Internet ;*
- *un agent qui emporte des informations (contenant des données) pour les utiliser dans le cadre de ses nouvelles fonctions sans y être autorisé.*

les **violations de disponibilité** : il s'agit des cas de perte d'accès ou de destruction accidentelle ou non autorisée de données.

Exemples :

- *destruction erronée de documents papier contenant des données non autrement disponibles;*
- *suppression accidentelle d'un fichier de données en l'absence de sauvegarde ;*
- *perte d'accès aux données en raison d'un ransomware.*

3

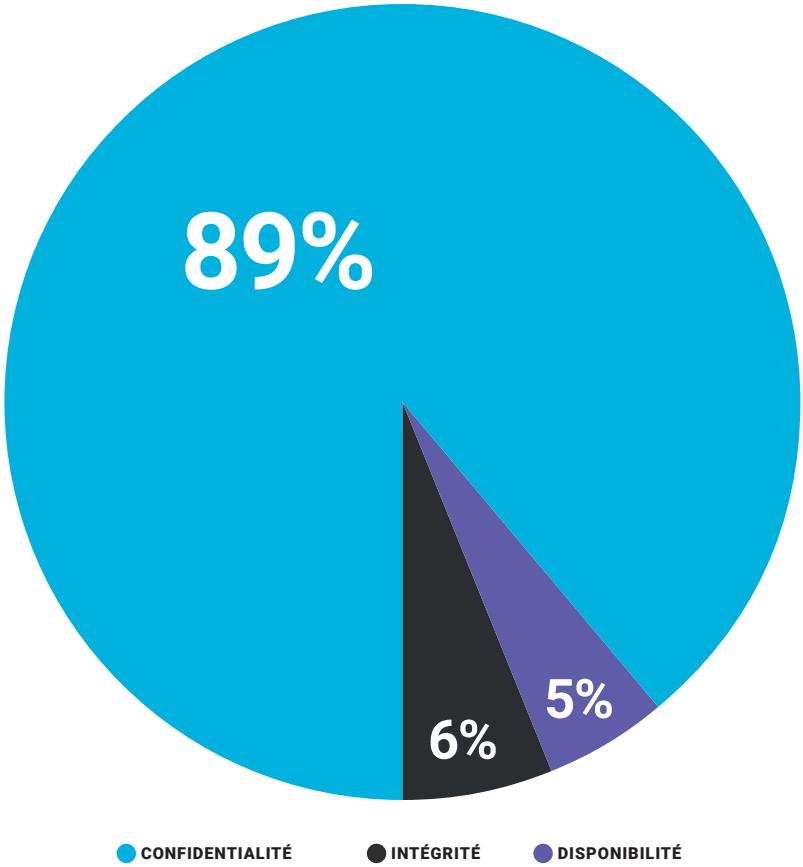
les **violations d'intégrité** : ce sont les cas où les données ont été modifiées de manière non autorisée ou accidentelle.

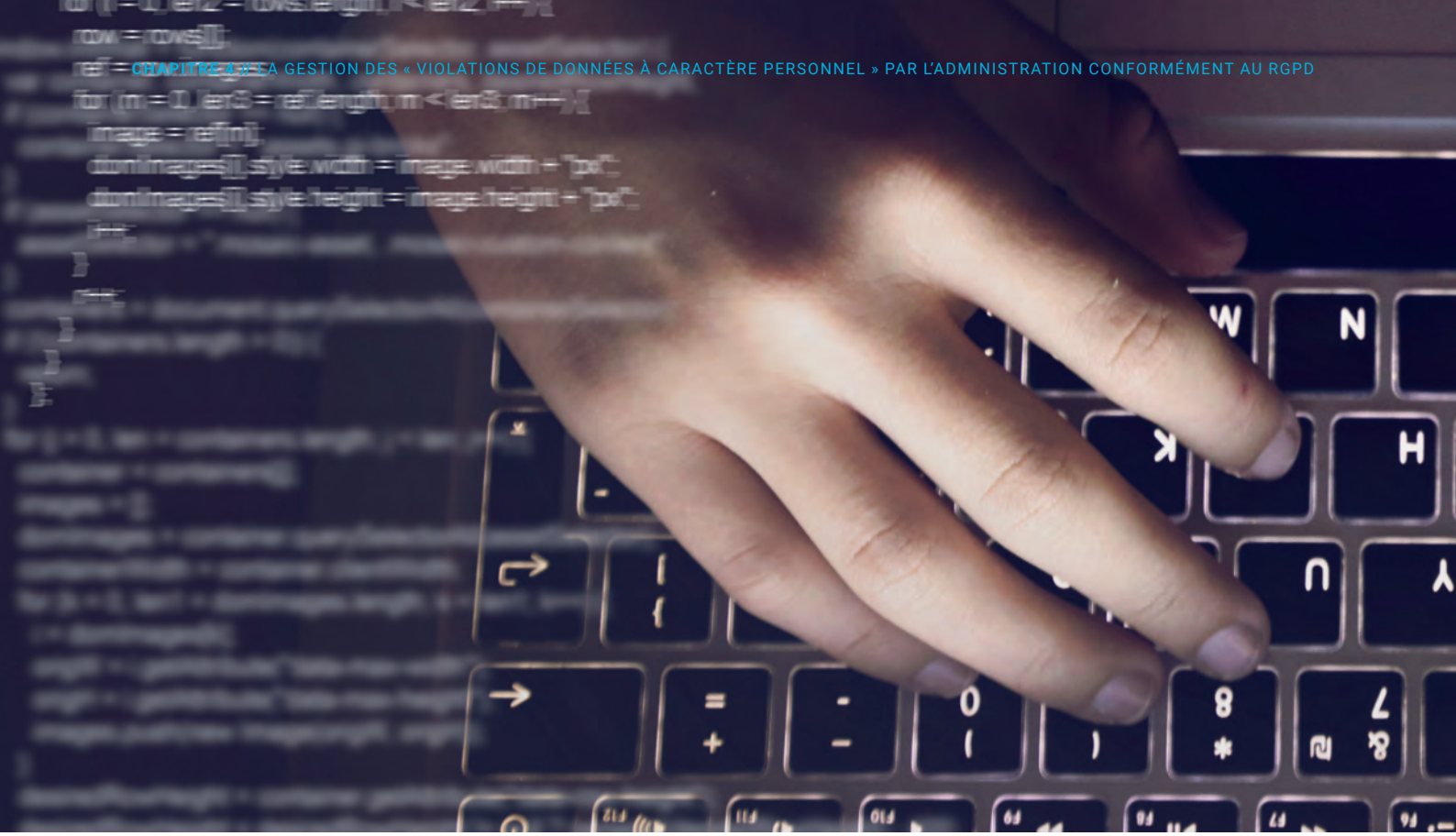
Exemples :

- *mauvaise manipulation de données dans un fichier par un agent ;*
- *remplacement des données par des informations incorrectes en raison d'une erreur dans le système informatique ;*
- *modification intentionnelle des données par un tiers via un programme malveillant (malware).*

Une violation de données peut concerner un seul de ces types d'incidents, ou en combiner plusieurs à la fois. Toutefois, on observe que la grande majorité des violations de données consistent en une violation de la confidentialité.

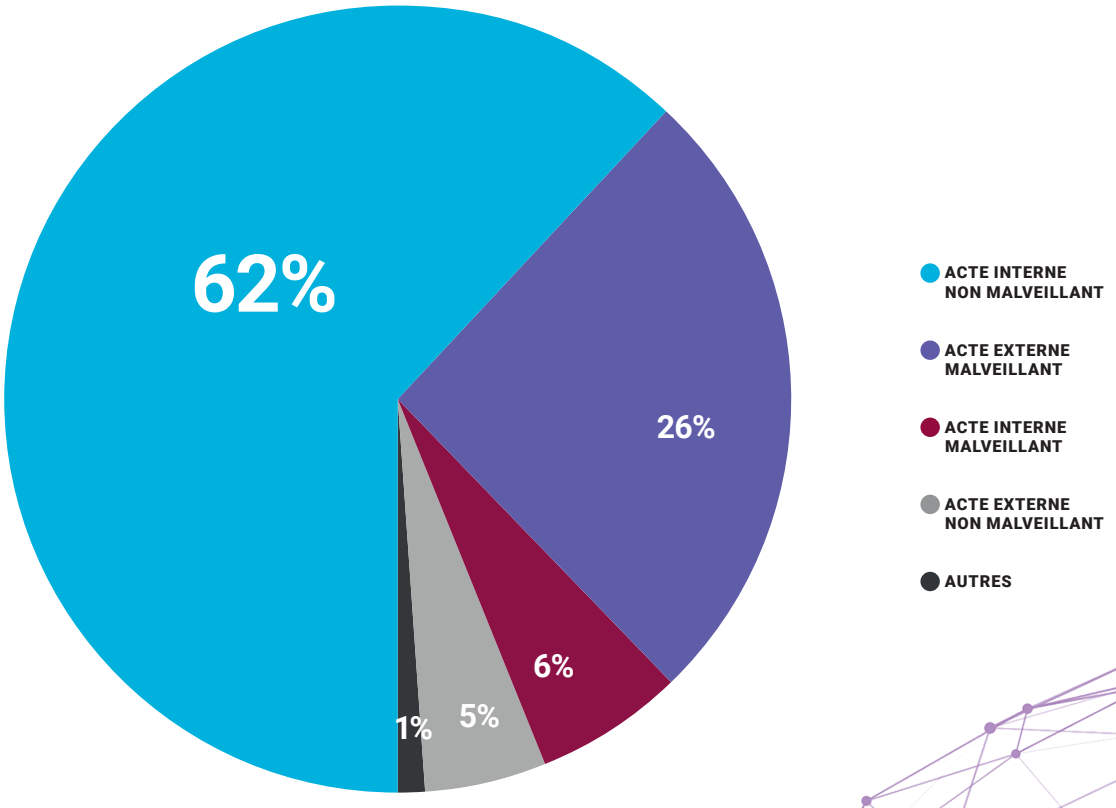
En 2021, les violations de données notifiées à la CNPD concernaient :

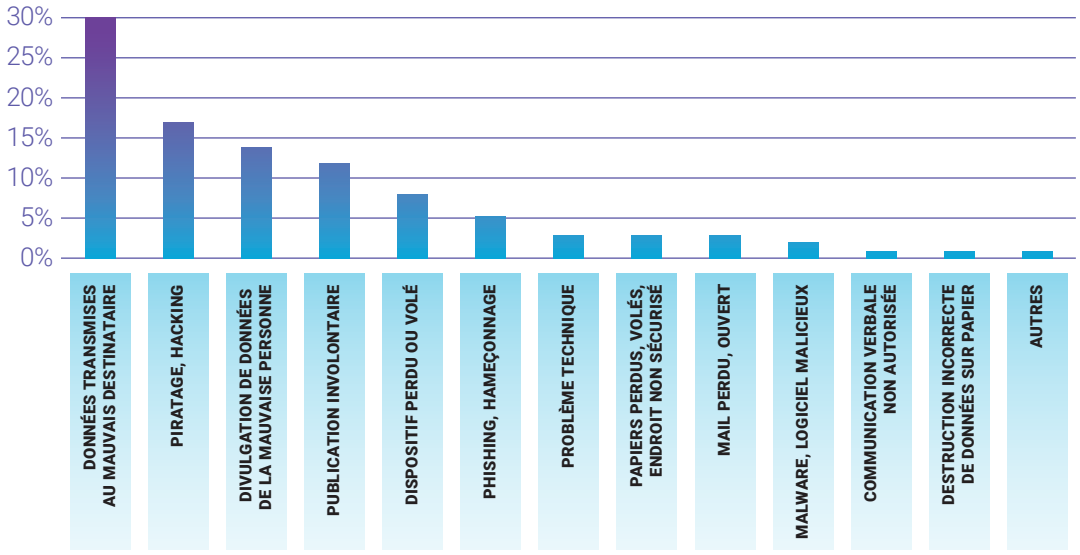




LES PRINCIPALES CAUSES DES VIOLATIONS DE DONNÉES

En 2021, 333 violations de données à caractère personnel ont été notifiées à la CNPD :





Les notifications transmises à la CNPD font distinctement apparaitre que la principale cause des violations de données reste l'erreur humaine (62% des violations concernent un acte interne non malveillant en 2021).

La CNPD énumère dans son rapport annuel 2021, les erreurs humaines les plus courantes, parmi lesquelles se retrouvent :

- la mauvaise application d'une procédure existante ou d'une règle de sécurité,
- l'absence ou l'insuffisance de sensibilisation aux règles de confidentialité à respecter,
- l'erreur d'inattention.

La seconde cause des violations de données à caractère personnel en 2021 sont les actes externes malveillants (26% des violations de données notifiées à la CNPD). Ces violations se distinguent des premières, car elles présentent bien souvent un impact plus important et un risque a priori plus élevé pour les personnes concernées.

SECTION 2 :
L'ADMINISTRATION EN CHARGE DE LA GESTION DES VIOLATIONS DE DONNÉES

L'obligation de gérer les violations des données conformément au RGPD incombe à l'administration responsable du traitement des données.

Un élément clé de toute politique de sécurité des données consiste en la description tant de mesures destinées à prévenir les violations de données que de mesures visant à réagir le plus vite possible en cas de violation.

Conformément au principe d'« accountability » du RGPD, l'administration responsable du traitement ne doit pas seulement assurer le respect du RGPD, mais elle doit également être en mesure de démontrer que celui-ci est respecté.

Dans cette optique, l'administration doit documenter la mise en place de ces mesures pour la sauvegarde des droits et libertés des personnes concernées, y compris pour la gestion des violations de données.

A noter que **le sous-traitant est tenu de signaler toute violation au responsable du traitement dans les meilleurs délais après en avoir pris connaissance**. Par ailleurs, il est tenu d'aider le responsable du traitement à garantir ses obligations en matière de gestion des violations de données.

SECTION 3 :
LE NIVEAU DE « RISQUE » COMME FACTEUR DÉTERMINANT DES SUITES À DONNER À UNE VIOLATION DE DONNÉES

Une violation de données risque, si l'on n'intervient pas à temps et de manière appropriée, de causer aux personnes physiques concernées des dommages physiques, matériels ou un préjudice moral.

Parmi les dommages physiques, matériels et moraux listés par le RGPD, on retrouve :

UNE DISCRIMINATION

UNE PERTE DE CONFIDENTIALITÉ DE DONNÉES PROTÉGÉES PAR LE SECRET PROFESSIONNEL

UNE USURPATION D'IDENTITÉ

UN VOL OU UNE PERTE FINANCIÈRE

UNE ATTEINTE À LA RÉPUTATION

UNE PERTE DE CONTRÔLE DES PERSONNES CONCERNÉES SUR LEURS DONNÉES

UNE LIMITATION DANS L'EXERCICE DES DROITS DES PERSONNES CONCERNÉES

La référence aux droits et libertés des personnes physiques vise principalement les droits à la protection des données et au respect de la vie privée. Elle s'étend toutefois à d'autres droits fondamentaux qui sont reconnus à chaque individu comme, notamment, la liberté d'expression, la liberté de pensée, l'interdiction de toute discrimination, le droit à la liberté de conscience et de religion ainsi que la liberté de circulation.

Le RGPD prévoit **3 niveaux de risques** potentiels qu'une violation de données peut engendrer pour les droits et libertés de la personne concernée (« risque ») :

- la violation **n'est pas susceptible d'engendrer un risque,**
- la violation **est susceptible d'engendrer un risque,**
- la violation **est susceptible d'engendrer un risque élevé.**

En fonction du niveau de risque identifié par l'administration, cette dernière doit entreprendre des démarches différentes. Ainsi, si une violation de données :

- **n'est pas susceptible d'engendrer un risque**, il suffit que l'administration la documente en interne.

- **est susceptible d'engendrer un risque**, l'administration doit :
  - la documenter en interne, et
  - la notifier à la CNPD.

- **est susceptible d'engendrer un risque élevé**, l'administration doit :
  - la documenter en interne,
  - la notifier à la CNPD, et
  - la communiquer à la personne concernée.

	Documenter en interne	Notifier à l'autorité de contrôle	Communiquer à la personne concernée
Aucun risque	✓	✗	✗
Risque	✓	✓	✗
Risque élevé	✓	✓	✓

(pour de plus amples explications sur la documentation par le responsable du traitement, la notification à la CNPD, la communication à la personne concernée, voir *infra*.)

SECTION 4 : L'ÉVALUATION OBJECTIVE DU RISQUE

L'administration est tenue d'évaluer le risque lié à une violation de données de manière objective, en particulier en termes d'impact et de probabilité.

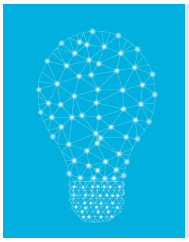
Le RGPD ne précise aucune méthodologie pour évaluer les risques causés par une violation de données, de sorte que l'administration est libre de choisir la méthode qu'elle souhaite utiliser. Cela étant dit, la méthode choisie doit, conformément au principe d'« accountability », répondre aux conditions minimales en termes d'objectivité de l'évaluation du risque et comporter une documentation des décisions prises.

Dans un objectif de mise en œuvre cohérente des politiques dans le domaine de la protection des données, et afin de guider et accompagner les administrations dans cet exercice, **le CGPD propose** de baser l'évaluation du risque sur :

- des critères « objectifs »,
- des facteurs aggravants et atténuants,
- une appréciation souveraine par l'administration du risque encouru par la personne concernée du fait de la violation des données.

Les critères et éléments proposés par le CGPD ont été élaborés en tenant compte de la guidance, en particulier des autorités de contrôle, de l'EDPB, de l'ENISA ainsi que des entités nationales compétentes en matière de sécurité de l'information. Ils ne prétendent pas à l'exhaustivité.

Dans un objectif d'approche cohérente, **le CGPD met également à disposition des administrations un outil d'assistance** qui permet de réaliser une évaluation préliminaire du risque.



Cet outil ne dispense toutefois pas les administrations d'assurer une évaluation complète et circonstanciée du risque et d'entamer les démarches nécessaires conformément au RGPD (documenter la violation et, le cas échéant, notifier la violation à l'autorité de contrôle et la communiquer aux personnes concernées).

LES CRITÈRES OBJECTIFS À PRENDRE EN COMPTE

Pour évaluer le risque, le CGPD propose aux administrations de tenir compte de plusieurs critères objectifs.

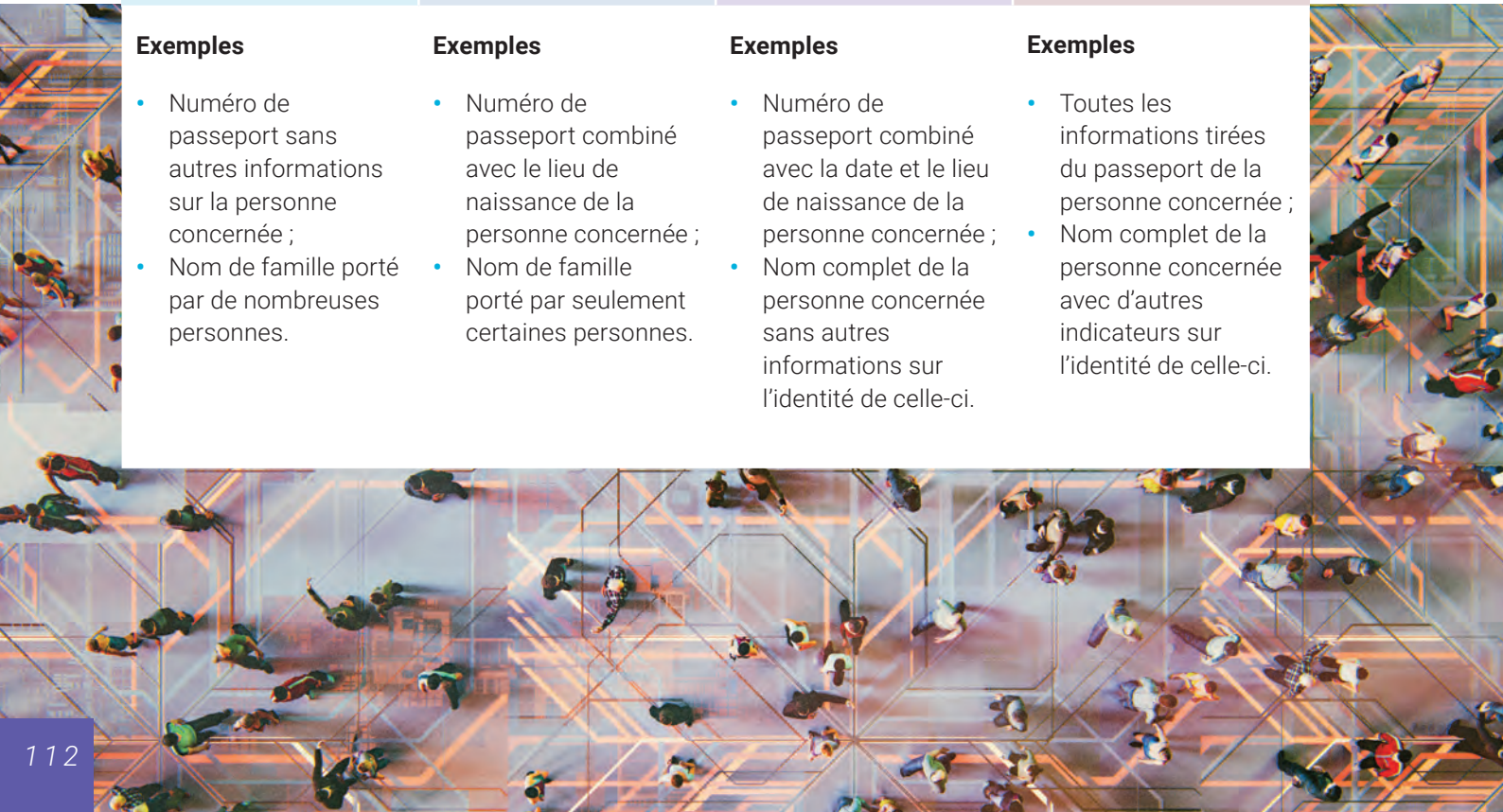
Pour chaque critère, l'administration doit évaluer si le risque est « négligeable », « limité », « important », voire « maximal ».

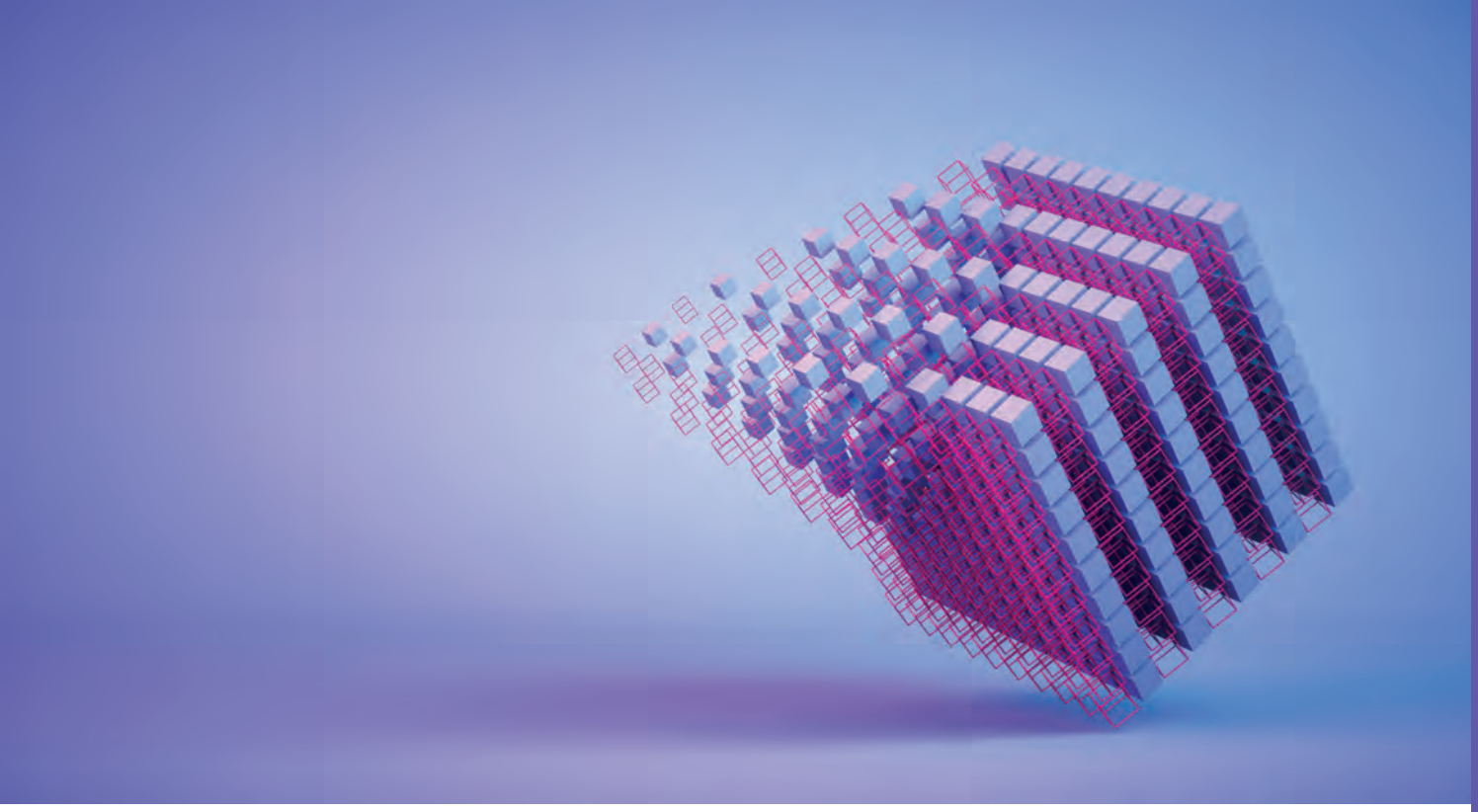
1 La facilité d'identification des personnes concernées

L'administration doit **évaluer la facilité avec laquelle les personnes concernées peuvent être identifiées à l'aide des données touchées par la violation de données**.

A noter, à titre d'illustration, que les données protégées par un niveau de cryptage approprié sont, a priori, incompréhensibles pour un tiers qui n'est pas en possession de la clé de décryptage. Une mesure de pseudonymisation peut également réduire (mais non pas exclure) la probabilité que l'individu soit identifié en cas de violation de données.

RISQUE NÉGLIGEABLE	RISQUE LIMITÉ	RISQUE IMPORTANT	RISQUE MAXIMAL
Il semble quasiment impossible d'identifier les personnes à l'aide des données concernées par la violation	**Il semble difficile d'identifier les personnes à l'aide des données concernées, bien que cela soit possible dans certains cas**	**Il semble relativement facile d'identifier les personnes à l'aide des données concernées**	**Il semble certain d'identifier les personnes à l'aide des données concernées**
Exemples • Numéro de passeport sans autres informations sur la personne concernée ; • Nom de famille porté par de nombreuses personnes.	**Exemples** • Numéro de passeport combiné avec le lieu de naissance de la personne concernée ; • Nom de famille porté par seulement certaines personnes.	**Exemples** • Numéro de passeport combiné avec la date et le lieu de naissance de la personne concernée ; • Nom complet de la personne concernée sans autres informations sur l'identité de celle-ci.	**Exemples** • Toutes les informations tirées du passeport de la personne concernée ; • Nom complet de la personne concernée avec d'autres indicateurs sur l'identité de celle-ci.





2 La nature et la sensibilité des données

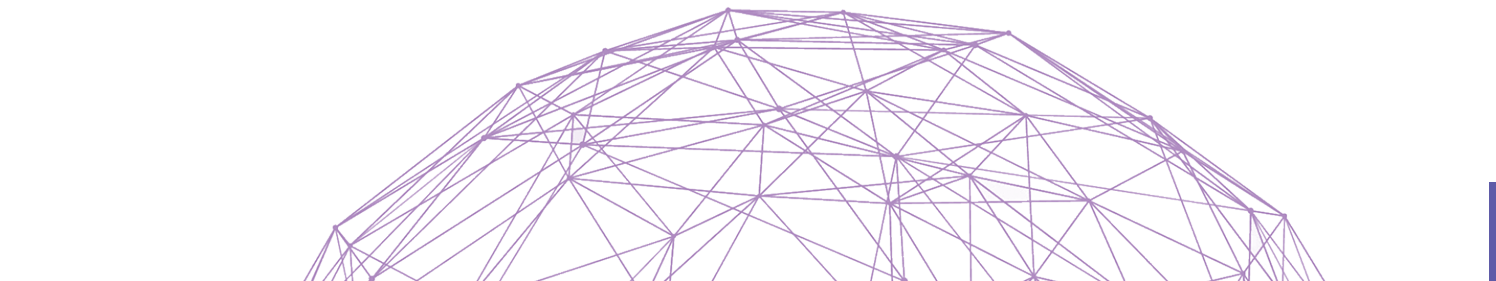
Plus les données sont sensibles, plus le risque sera élevé.

L'administration doit évaluer ce que les données révèlent sur la personne concernée (ex. : une combinaison de données permet de tirer plus de conclusions qu'une donnée prise isolément).

Par ailleurs, l'article 9 du RGPD prévoit des catégories particulières de données pour lesquelles s'appliquent des conditions particulières de traitement compte tenu de leur sensibilité (« données sensibles »).

Constituent des données sensibles au regard du RGPD :

- LES ORIGINES RACIALES OU ETHNIQUES
- LES OPINIONS POLITIQUES
- LES CONVICTIONS RELIGIEUSES OU PHILOSOPHIQUES
- L'APPARTENANCE SYNDICALE
- LA SANTÉ (PHYSIQUE OU MENTALE)
- LA VIE SEXUELLE OU L'ORIENTATION SEXUELLE
- LES DONNÉES GÉNÉTIQUES
- LES DONNÉES BIOMÉTRIQUES



L'article 10 du RGPD prévoit, en outre, des conditions spécifiques quant au traitement des données relatives aux condamnations pénales et aux infractions.




RISQUE NÉGLIGEABLE	RISQUE LIMITÉ	RISQUE IMPORTANT	RISQUE MAXIMAL
Données à caractère personnel ordinaires	**Données ordinaires qui donnent une indication sur les préférences de la personne concernée**	**Données financières ou donnant une indication sur le comportement de la personne concernée**	**Catégories particulières de données (art. 9 et 10 du RGPD tels que détaillées *supra*)**
Exemples • *Données d'identification ;* • *Adresse de la personne concernée.*	**Exemples** • *Données donnant une indication sur les préférences gastronomiques ;* • *Données sur les déplacements touristiques de la personne concernée.*	**Exemples** • *Informations sur la rémunération ou concernant des transactions financières (ex. : relevés bancaires) ;* • *Informations concernant le patrimoine d'une personne concernée (ex. : possession immobilière).*	**Exemples** • *Données concernant les opinions politiques, les convictions religieuses ou philosophiques de la personne concernée ;* • *Données de santé.*

Le volume de données et la durée de la violation

Le fait qu'une violation impacte une grande quantité de données et/ou qu'elle perdure sur une durée prolongée est un facteur aggravant.

En revanche, plus le volume de données touchées par la violation est petit et le temps de cette dernière réduite, moins le risque est élevé.




RISQUE NÉGLIGEABLE	RISQUE LIMITÉ	RISQUE IMPORTANT	RISQUE MAXIMAL
Courte période et petit volume de données concernées	**Longue période et petit volume de données concernées**	**Courte période et grand volume de données concernées**	**Longue période et grand volume de données concernées**

Les caractéristiques particulières des personnes concernées

Le degré de vulnérabilité des individus auxquels se rapportent les données touchées par la violation des données doit être pris en considération par l'administration lors de l'évaluation du risque.

Le risque engendré par une violation est plus important si elle concerne des données relatives à des enfants ou d'autres personnes vulnérables.

RISQUE NÉGLIGEABLE	RISQUE LIMITÉ	RISQUE IMPORTANT	RISQUE MAXIMAL
Des personnes « ordinaires »	**Un groupe social particulier**	**Des personnes exposées publiquement**	**Des mineurs et/ou d'autres personnes vulnérables**
Exemples • *Tous les contribuables du pays ;* • *Tous les résidents de la commune.*	**Exemples** • *Les membres d'un club de sport ;* • *Les participants à un événement spécifique.*	**Exemples** • *Les artistes connus par le grand public ;* • *Les responsables politiques d'une commune.*	**Exemples** • *Des enfants ;* • *Des personnes en situation de handicap.*

Le nombre de personnes concernées par la violation de données

En général, plus le nombre de personnes concernées par la violation de données est important, plus le risque engendré par celle-ci est élevé.

RISQUE NÉGLIGEABLE	RISQUE LIMITÉ	RISQUE IMPORTANT	RISQUE MAXIMAL
Un individu	**Un petit groupe d'individus**	**Un grand groupe d'individus**	**La totalité d'une catégorie d'individus**

LES FACTEURS ATTÉNUANTS OU AGGRAVANTS

Dans le cadre de l'évaluation du risque engendré par une violation de données, l'administration doit également **tenir compte de plusieurs facteurs atténuants (réduisant le risque) et aggravants (élevant le risque)**.

Sont considérés comme **facteurs atténuants**, le fait que :

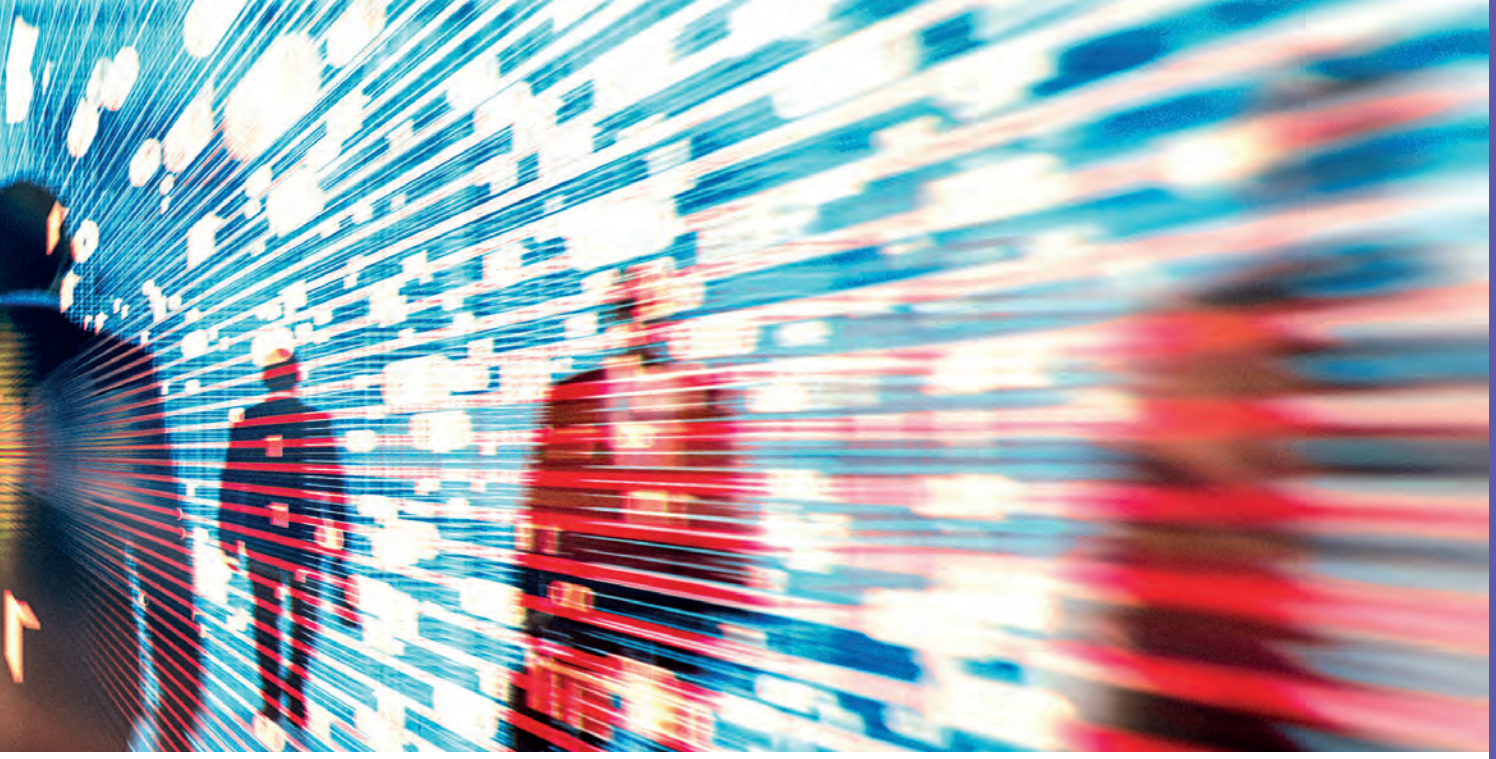
- **LES DONNÉES ÉTAIENT PUBLIQUEMENT ACCESSIBLES**
- **LES DONNÉES ONT ÉTÉ TRANSMISES PAR ERREUR À UN TIERS DIGNE DE CONFIANCE**
- **LES DONNÉES SONT PROTÉGÉES PAR CHIFFREMENT DE POINTE**

Sont considérés comme **facteurs aggravants**, le fait que :

- **LES DONNÉES SONT TRANSMISES À UN NOMBRE INCONNU DE DESTINATAIRES**
- **LES DONNÉES SONT IRRÉMÉDIABLEMENT PERDUES**
- **LA VIOLATION EST DUE À UNE INTENTION MALVEILLANTE, FRAUDULEUSE OU CRIMINELLE**

L'APPRÉCIATION SOUVERAINE DU RISQUE PAR LE RESPONSABLE DU TRAITEMENT

En complément des critères objectifs et des facteurs atténuants ou aggravants (voir *supra*), **l'administration doit apprécier souverainement le risque** encouru par la violation de données.



A cette fin, l'administration devrait notamment prendre en compte les éléments suivants :

1

Le type de violation de données

Le type de la violation de données survenue (violation de confidentialité, violation de disponibilité, violation d'intégrité) a une incidence sur le niveau de risque.

En effet, il est généralement accepté qu'une violation de la confidentialité a des conséquences plus graves qu'une indisponibilité temporaire des données. Or, cette appréciation doit se faire au cas par cas en tenant compte, notamment, du contexte et des circonstances concrètes de la situation (ex. : une indisponibilité du dossier patient au cours d'une chirurgie peut entrainer des conséquences plus graves que la consultation erronée du même dossier par un professionnel de santé non concerné travaillant au sein du même hôpital).

Dans ce même ordre d'idées, une violation de données consistant tant en une violation de la confidentialité, de la disponibilité, que de l'intégrité a des conséquences plus graves qu'une seule violation de l'intégrité des données.

2

Les caractéristiques particulières du responsable du traitement

Le rôle de l'administration et la nature de ses activités peuvent affecter le niveau de risque dès lors que ces éléments peuvent donner lieu à des indications supplémentaires sur la situation de la personne concernée.

La gravité des conséquences pour les personnes concernées

Le risque varie au cas par cas en fonction des circonstances concrètes de la violation de données.

Pour ces motifs, l'administration doit évaluer, notamment, si la violation de données peut entraîner, entre autres :

- un vol ou une usurpation d'identité,
- un préjudice physique,
- une détresse psychologique,
- une humiliation,
- une atteinte à la réputation.

Les intentions inconnues ou potentiellement malicieuses des destinataires (ex. : une attaque de « phishing ») ou le fait que le destinataire puisse être considéré comme « fiable » (ex. : un agent envoie des données à un autre agent de son administration) sont également à prendre en considération.

NIVEAU DE RISQUE SOUVERAINEMENT APPRÉCIÉ PAR L'ADMINISTRATION

RISQUE NÉGLIGEABLE	RISQUE LIMITÉ	RISQUE IMPORTANT	RISQUE MAXIMAL
Les personnes concernées ne seront pas impactées ou pourraient connaître seulement quelques légers désagréments, qu'elles surmonteront sans difficulté	**Les personnes concernées pourraient connaître des désagréments, qu'elles pourraient surmonter malgré quelques difficultés**	**Les personnes concernées pourraient connaître des conséquences significatives, qu'elles pourraient surmonter, mais avec de sérieuses difficultés**	**Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables et il est possible qu'elles ne puissent pas les surmonter**
Exemples • *Perte de temps pour réitérer des démarches ;* • *Attente supplémentaire, mais négligeable ;* • *Enervement.*	**Exemples** • *Frais supplémentaires ;* • *Refus d'accès temporaire à un service ;* • *Affection psychologique mineure.*	**Exemples** • *Détournements d'argent ou dégradation de biens ;* • *Perte de chance d'emploi ;* • *Affection physique ou psychologique d'une certaine gravité.*	**Exemples** • *Incapacité ou impossibilité de trouver un emploi ;* • *Péril financier ;* • *Affection psychologique ou physique de longue durée ou permanente.*

SECTION 5 :
LA DOCUMENTATION INTERNE DE LA VIOLATION DE DONNÉES

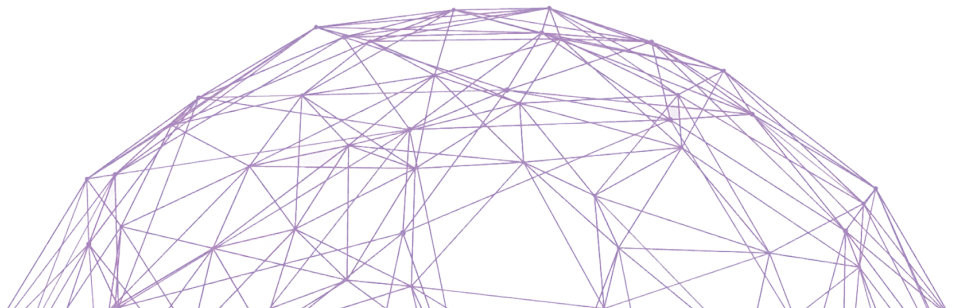
LE CONTENU DE LA DOCUMENTATION INTERNE

L'administration responsable du traitement de données doit **documenter toute violation de données en interne.**

Pour ce faire, elle doit établir un registre interne des violations qui doit comprendre, pour chaque violation de données, en particulier, les informations suivantes :

- une description des faits relatifs à la violation ;
- la nature de la violation de données, y compris si possible, les catégories et le nombre approximatif de personnes concernées ainsi que les catégories et le nombre approximatif d'enregistrements de données concernés ;
- une description des mesures prises ou proposées par l'administration pour remédier à la violation de données et pour en atténuer les éventuelles conséquences négatives ;
- une description des effets et des conséquences probables de la violation de données ;
- le nom et les coordonnées du DPD ou d'un autre point de contact auprès duquel des informations supplémentaires concernant la violation de données peuvent être obtenues ;
- l'évaluation du risque faite par l'administration ainsi que le raisonnement justifiant les décisions prises en réaction à la violation de données, en particulier lorsqu'une violation n'est pas notifiée à la CNPD (ou notifiée avec retard) ou n'est pas communiquée à la personne concernée ;
- si applicable, la preuve de la notification de la violation à l'autorité de contrôle et de sa communication à la personne concernée.

Le registre des violations, établi dans une optique d'« accountability », peut servir de justificatif en cas de contrôle de la CNPD. Il doit donc permettre de démontrer le respect des exigences du RGPD, en reprenant notamment les éléments factuels de la violation de données, les décisions prises par le responsable du traitement, ainsi que la motivation de ces dernières.

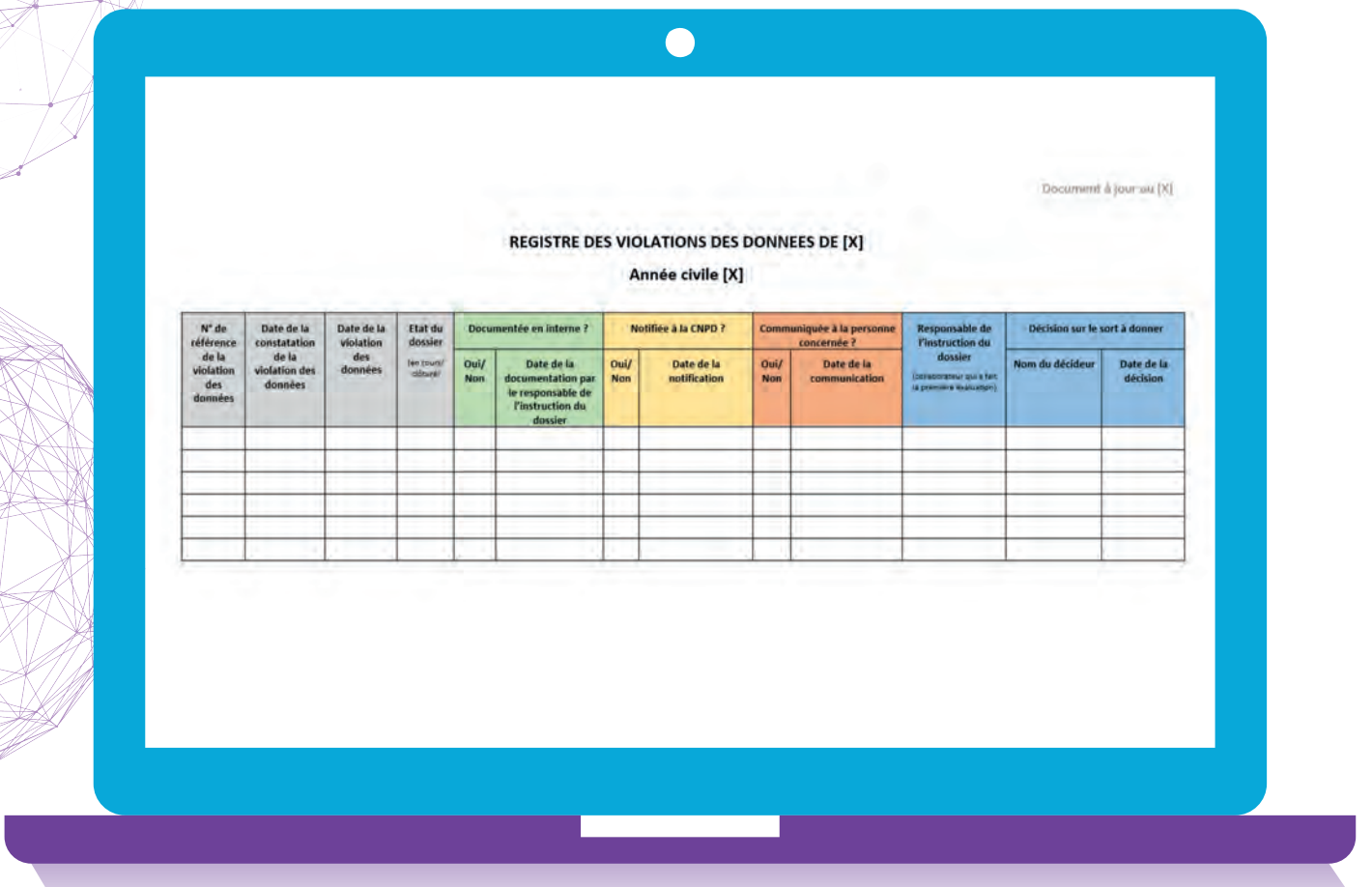


LA FORME DE LA DOCUMENTATION INTERNE

L'administration est libre de déterminer la méthode et la structure à utiliser pour documenter les violations de données en interne. En effet, le RGPD n'impose pas un format standardisé. Cela étant dit, la méthode choisie doit répondre aux conditions de documentation exigées par le RGPD en termes d'« accountability » du responsable du traitement.

Dans un objectif de guider et accompagner les administrations dans cet exercice, **le CGPD propose** de recenser :

- l'ensemble des principaux éléments relatifs aux violations de données dans un registre centralisé des violations de données. Ce registre pourra notamment prendre la forme suivante :



Document à jour au [X]

REGISTRE DES VIOLATIONS DES DONNEES DE [X]

Année civile [X]

N° de référence de la violation des données	Date de la constatation de la violation des données	Date de la violation des données	Etat du dossier (en cours/clôturé)	Documentée en interne ?		Notifiée à la CNPD ?		Communiquée à la personne concernée ?		Responsable de l'instruction du dossier (personne qui a fait la première évaluation)	Décision sur le sort à donner	
				Oui/ Non	Date de la documentation par le responsable de l'instruction du dossier	Oui/ Non	Date de la notification	Oui/ Non	Date de la communication		Nom du décideur	Date de la décision

- les détails de chaque violation de données (recensées dans le tableau ci-dessus) en s'appuyant sur le formulaire de notification établi par la CNPD (voir *infra* pour de plus amples informations).

Le formulaire de la CNPD - servant dans ce contexte de canevas - doit, dans le cas de la documentation interne, être complété par les informations spécifiques requises en matière de documentation, à savoir, le raisonnement justifiant les décisions prises par l'administration en réaction à la violation (en particulier l'évaluation du risque) et, si applicable, la preuve de la notification de la violation à la CNPD et de sa communication à la personne concernée.

SECTION 6 :
LA NOTIFICATION DE LA VIOLATION DE DONNÉES À LA CNPD

UNE OBLIGATION PESANT SUR LE RESPONSABLE DU TRAITEMENT

Dans l'hypothèse où la violation est susceptible d'engendrer un risque, l'administration doit, à la fois, documenter la violation en interne (voir *supra*) et notifier celle-ci à la CNPD.

L'obligation de notifier une violation incombe exclusivement à l'administration en sa qualité de responsable du traitement.

Le rôle du DPD se limite, en revanche, à informer et à conseiller le responsable du traitement sur les obligations qui lui incombent en vertu de la législation applicable en matière de protection des données et de faire office de point de contact pour la CNPD.

Le sous-traitant, pour sa part, doit signaler toute violation endéans les meilleurs délais au responsable du traitement et aider ce dernier à garantir le respect des obligations applicables en termes de gestion des violations des données, compte tenu de la nature du traitement et des informations à sa disposition. Le responsable du traitement peut demander au sous-traitant d'entreprendre les démarches préparatoires, mais la décision sur les suites à donner à la violation lui appartient toujours. L'assistance du sous-traitant ne dispense pas le responsable du traitement du respect des obligations mises à sa charge par le RGPD.

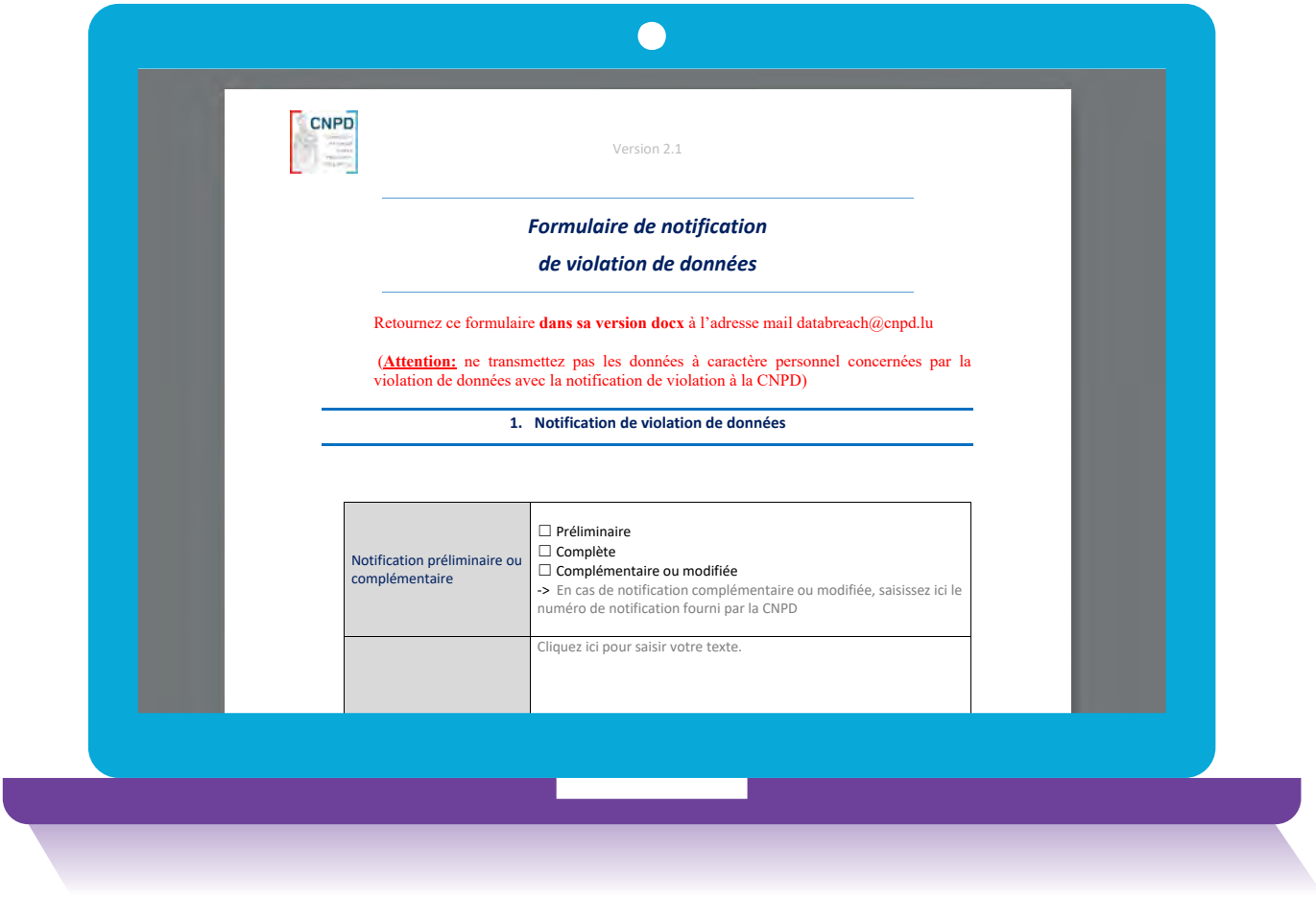
LES INFORMATIONS À NOTIFIER À LA CNPD

La notification à la CNPD doit, conformément à l'article 33 du RGPD, à tout le moins :

- décrire la nature de la violation de données 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 ;
- communiquer le nom et les coordonnées du DPD ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- décrire les conséquences probables de la violation de données ;
- décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Pour faciliter la notification de violations de données à son adresse, la CNPD a établi un formulaire de notification des violations des données.

Toute notification de violation doit se faire via le formulaire disponible sur le site Internet de la CNPD.



CNPD

Version 2.1

Formulaire de notification

de violation de données

Retournez ce formulaire **dans sa version docx** à l'adresse mail databreach@cnpd.lu

(**Attention:** ne transmettez pas les données à caractère personnel concernées par la violation de données avec la notification de violation à la CNPD)

1. Notification de violation de données

Notification préliminaire ou complémentaire	☐ Préliminaire ☐ Complète ☐ Complémentaire ou modifiée -> En cas de notification complémentaire ou modifiée, saisissez ici le numéro de notification fourni par la CNPD
	Cliquez ici pour saisir votre texte.

LE DÉLAI DE NOTIFICATION PRÉVU PAR LE RGPD

La notification à la CNPD doit être faite **dans les meilleurs délais et, au plus tard 72 heures après que l'administration a pris connaissance de la violation de données.**

Si l'administration ne notifie pas la violation de données dans les délais impartis, elle doit indiquer les motifs du retard dans la notification.

L'administration doit réagir à une alerte initiale et déterminer si une violation a effectivement eu lieu. Au cours de cette brève période, l'administration doit procéder à une enquête et collecter des preuves et autres informations pertinentes.

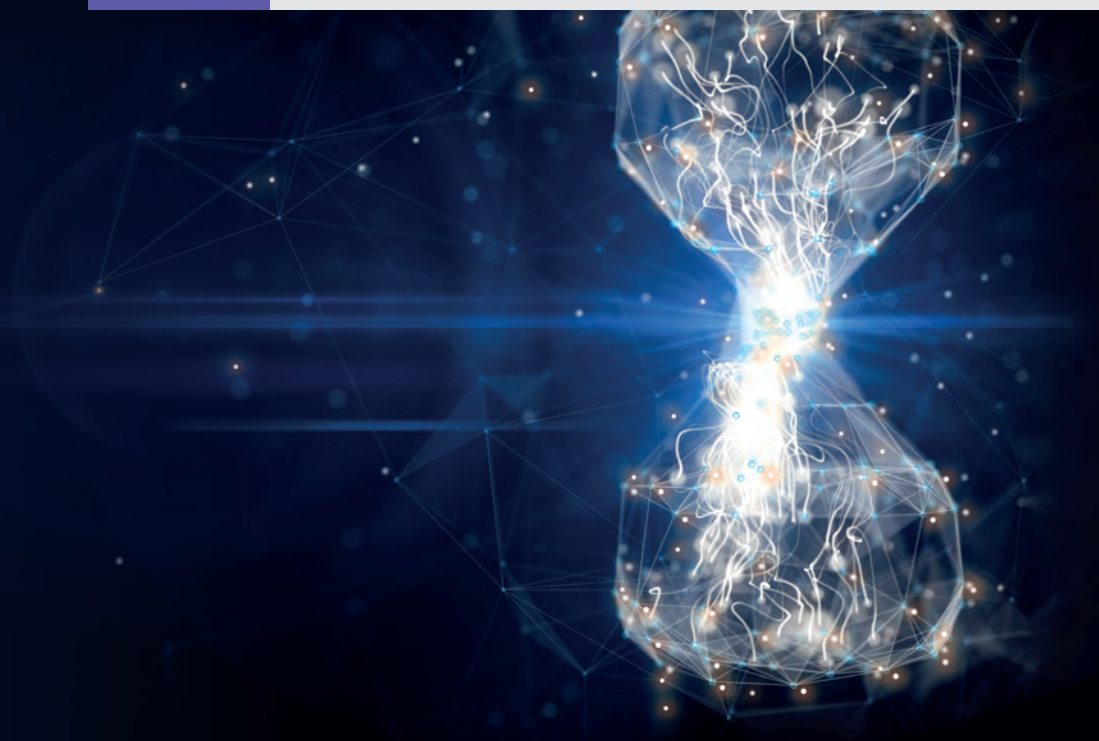
Une fois qu'elle a établi qu'une violation a eu lieu et qu'un risque (ou un risque élevé) a été identifié, l'administration doit notifier la violation à la CNPD dans les délais impartis.

La CNPD tient dans ce contexte à rappeler que :

- *le délai de 72 heures commence à courir à partir du moment où un agent de l'administration a « un doute raisonnable » sur l'existence d'une violation de données et non pas à partir du moment où le DPD a été mis au courant de la violation de données ;*
- *les jours fériés, les week-ends, les vacances, les maladies, etc. ne sont pas des motifs de retard acceptés par la CNPD ;*
- *l'administration doit veiller à ce que le processus de notification des violations de données ne dépende pas d'une seule personne.*

A noter que le formulaire de notification de la CNPD permet également au responsable du traitement de procéder à une notification préliminaire lorsque ce dernier ne peut pas récolter toutes les informations nécessaires dans le délai de 72 heures.

A noter également qu'aucune sanction n'est prévue en cas de notification à la CNPD d'un incident qui, en fin de compte, s'avère ne pas constituer une violation de données au sens du RGPD.



SECTION 7 :
LA COMMUNICATION DE LA VIOLATION DE DONNÉES À LA PERSONNE CONCERNÉE

UNE OBLIGATION À CHARGE DU RESPONSABLE DU TRAITEMENT

L'administration doit, conformément à l'article 34 du RGPD, communiquer une violation aux personnes concernées lorsqu'elle est susceptible d'engendrer un risque élevé.

La communication doit, en principe, se faire directement à l'individu au moyen de messages dédiés ne contenant pas d'autres informations. Elle doit se faire en des termes clairs et simples, de sorte à être aisément compréhensible par une personne non avertie.

Le responsable du traitement peut demander au sous-traitant d'entreprendre les démarches préparatoires, mais la décision sur les suites à donner à la violation appartient toujours au responsable du traitement. L'assistance du sous-traitant ne dispense pas le responsable du traitement du respect des obligations mises à sa charge par le RGPD.

L'administration doit déterminer le canal le plus approprié pour communiquer la violation aux personnes concernées. Elle doit choisir la méthode de communication qui maximise la probabilité que la personne concernée reçoive les informations afférentes (ex. : mail, SMS, message direct).

LE DÉLAI DE COMMUNICATION DE LA VIOLATION DE DONNÉES À LA PERSONNE CONCERNÉE

La communication d'une violation aux personnes concernées doit se faire **dans les meilleurs délais**, ce qui oblige l'administration à justifier et à documenter tout retard éventuel.

LES INFORMATIONS À COMMUNIQUER À LA PERSONNE CONCERNÉE

La communication d'une violation de données à la personne concernée doit au moins contenir les informations suivantes :

- une description de la nature de la violation,
- le nom et les coordonnées du DPD ou d'un autre point de contact,
- une description des conséquences probables de la violation de données pour la personne concernée,
- une description des mesures prises ou que l'administration propose de prendre pour remédier à la violation, y compris, le cas échéant, des mesures pour en atténuer les éventuelles conséquences négatives.

LES CONDITIONS DANS LESQUELLES LA COMMUNICATION N'EST PAS OBLIGATOIRE

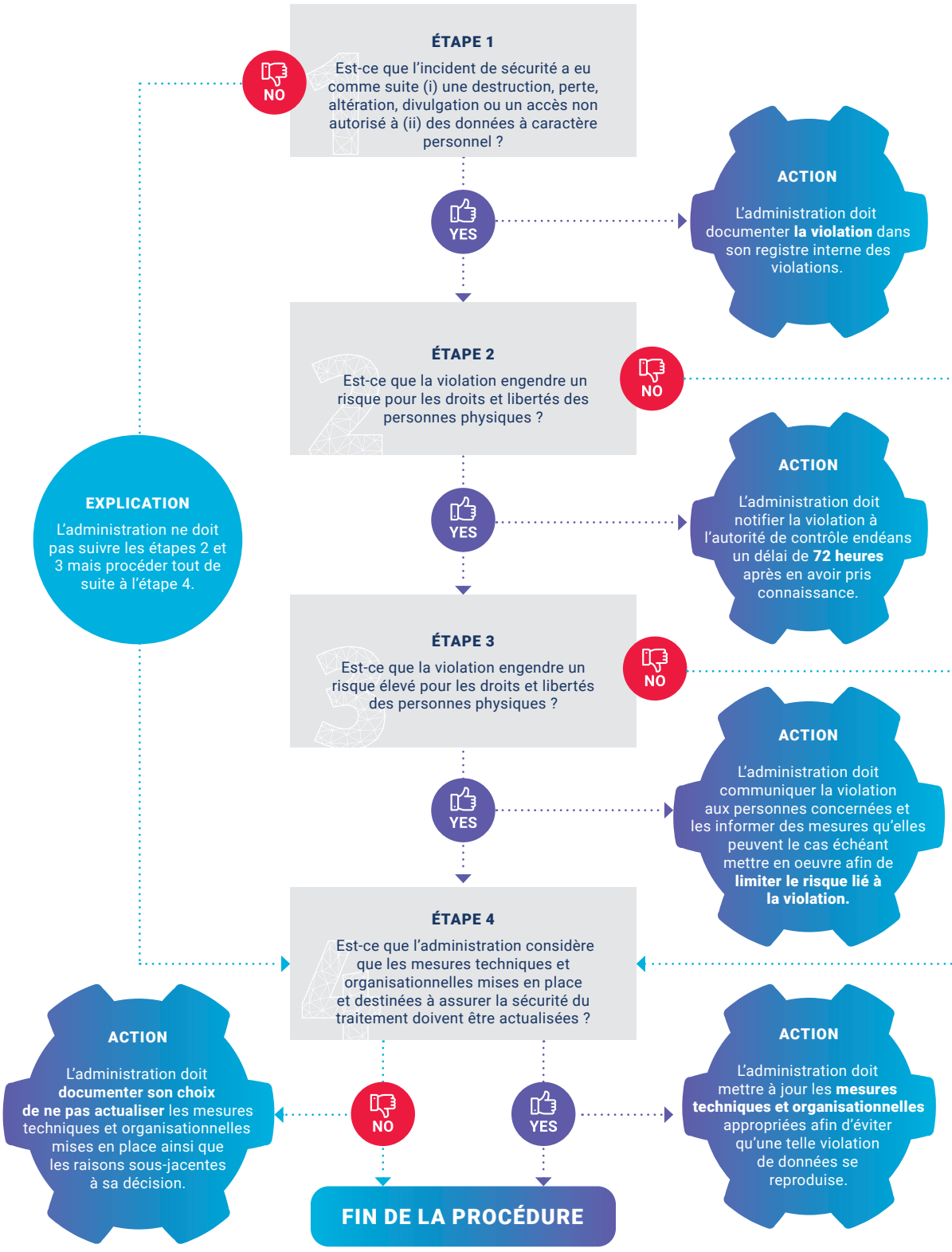
Il existe trois cas dans lesquels une communication à la personne concernée n'est pas requise alors même que la violation de données est susceptible d'engendrer un risque élevé :

- les données affectées par la violation de données ont, préalablement à cette dernière, été protégées par des mesures techniques et organisationnelles appropriées de sorte à être incompréhensibles pour des tiers (ex. : chiffrement de pointe des données enregistrées sur la clé USB perdue) ;
- l'administration a pris, immédiatement après la violation de données, des mesures qui garantissent que le risque élevé n'est plus susceptible de se concrétiser (ex. : les mots de passe des agents ayant accès à une base de données ont été subtilisés, mais ont été réinitialisés avant une quelconque utilisation par autrui) ;
- la communication à la personne concernée exigerait des efforts disproportionnés de la part de l'administration (ex. : l'administration ne dispose d'aucun élément permettant d'identifier directement les personnes concernées sans recours à des informations supplémentaires). Dans un tel cas, l'administration doit toutefois procéder à une communication publique ou prendre une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

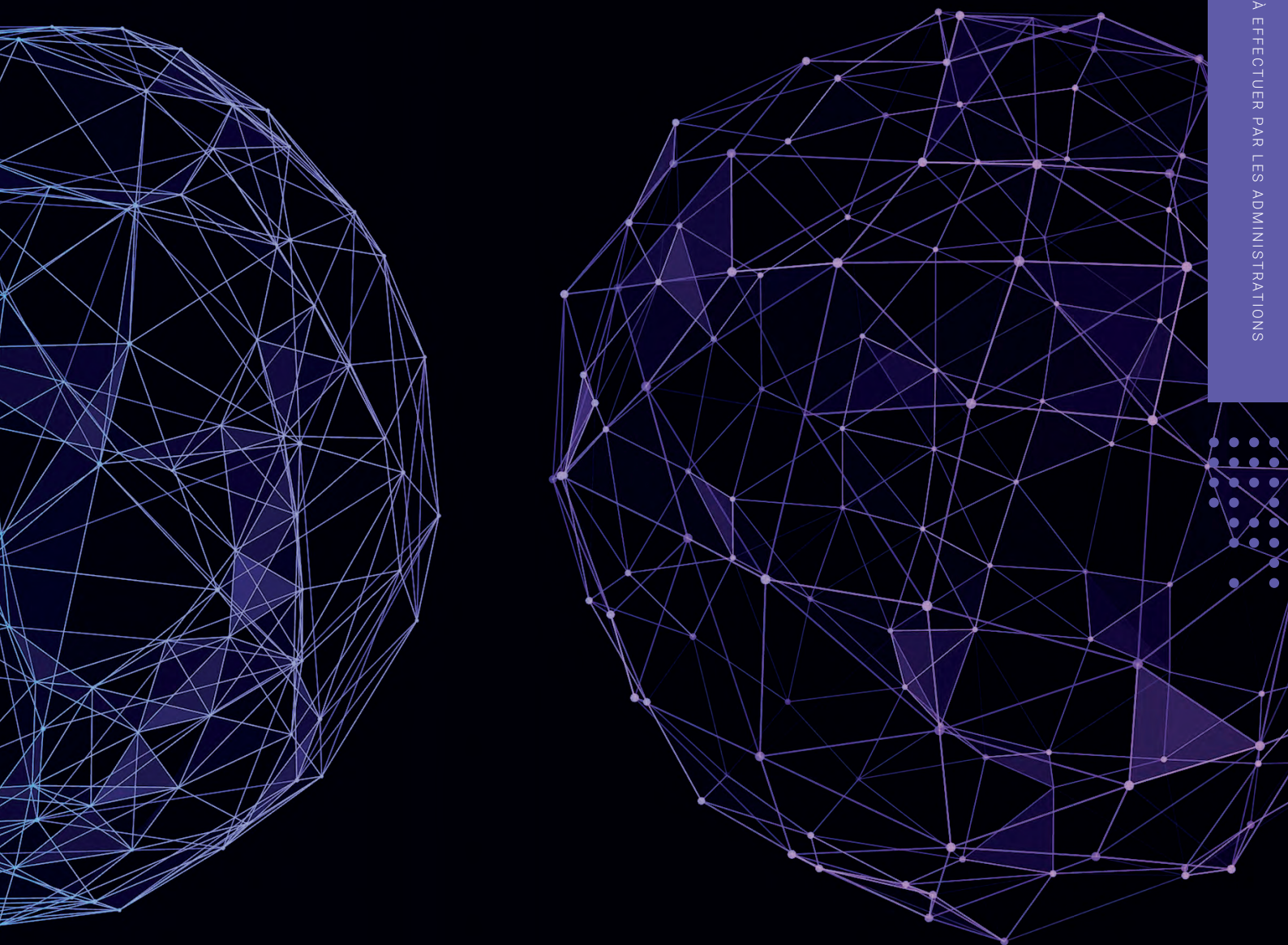
Notons que ces exceptions à l'obligation de communiquer une violation de données engendrant un risque élevé sont d'interprétation stricte. Conformément au principe d'accountability, l'administration doit être en mesure de démontrer à la CNPD qu'elle remplit les conditions de l'exception à l'obligation de communiquer qu'elle invoque.

SECTION 8 :
RÉCAPITULATIF DES ÉTAPES À SUIVRE

RÉCAPITULATIF DES ÉTAPES DE LA GESTION D'UNE VIOLATION DE DONNÉES PAR L'ADMINISTRATION



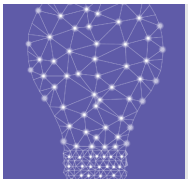
CHAPITRE 5 //
LES AUTRES TYPES DE NOTIFICATIONS D'INCIDENTS DE SÉCURITÉ À EFFECTUER PAR LES ADMINISTRATIONS



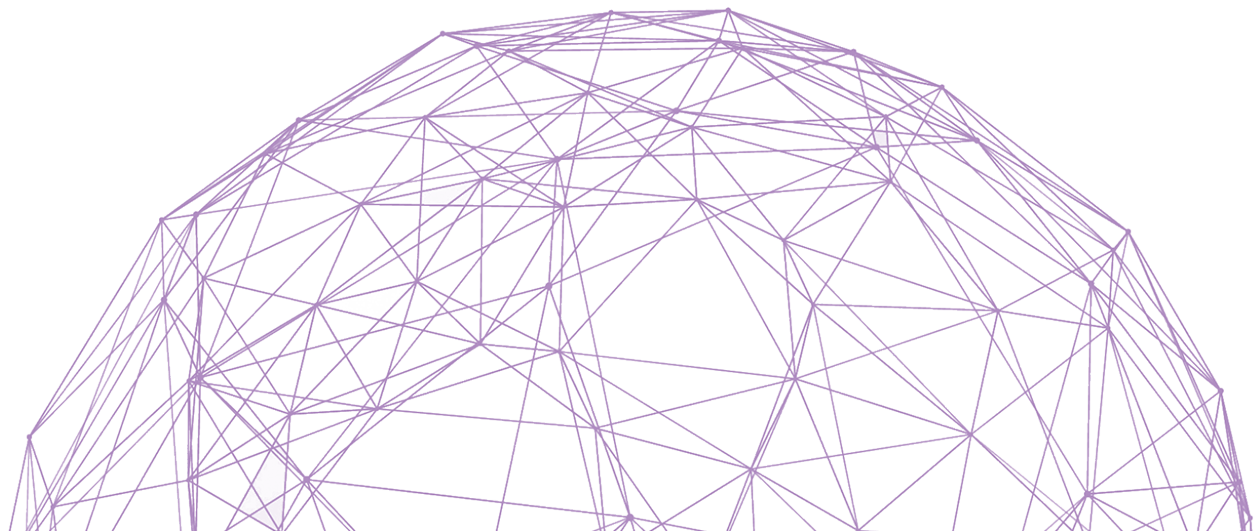
CHAPITRE 5 :
LES AUTRES TYPES DE NOTIFICATIONS D'INCIDENTS DE SÉCURITÉ À EFFECTUER PAR LES ADMINISTRATIONS

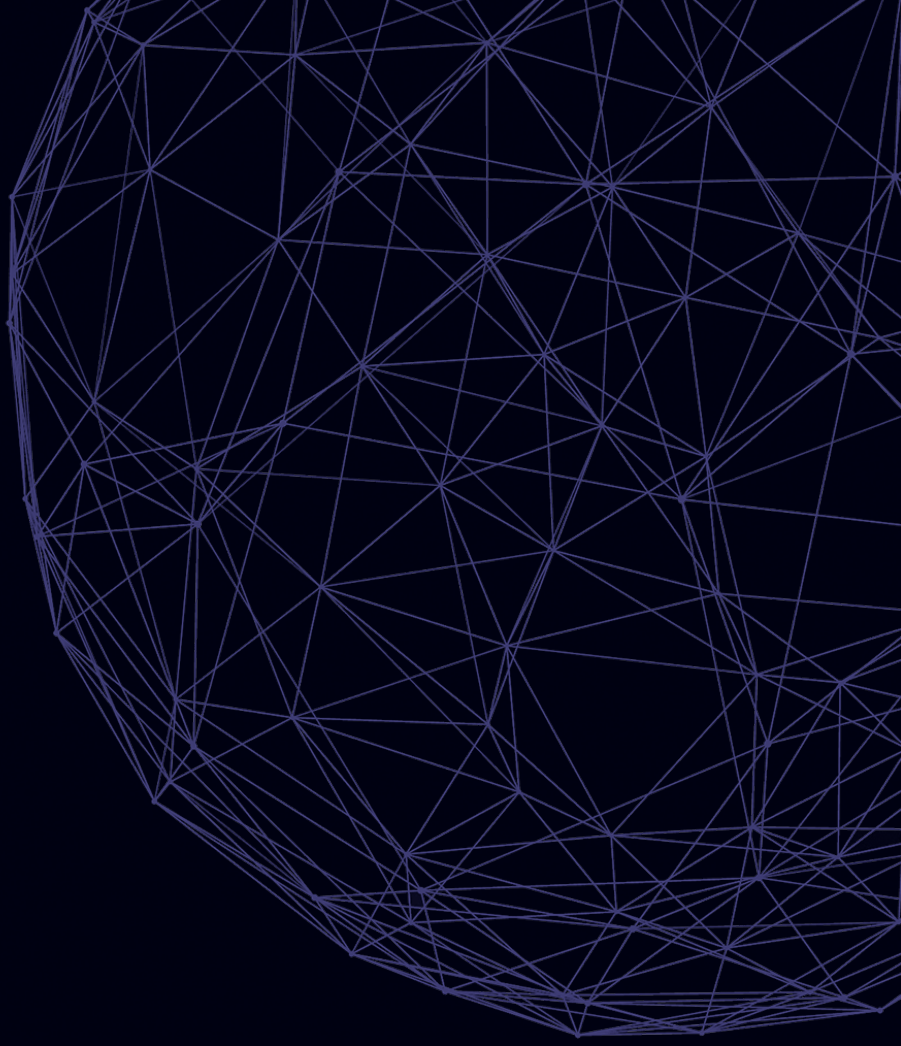
Outre la notification de la violation de données à la CNPD conformément au RGPD, l'administration peut être tenue de réaliser d'autres démarches ou notifications prévues par d'autres textes nationaux et européens applicables en matière de sécurité de l'information, telles que :

- la notification à l'ILR par les opérateurs de services essentiels relevant de sa compétence de tout incident ayant un impact significatif sur la continuité des services essentiels qu'ils fournissent (article 8 (4) de la loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant 1° la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat et 2° la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale) ;
- la notification à l'ILR par les fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public de tout incident de sécurité ayant un impact significatif sur le fonctionnement des réseaux ou des services (article 42 de la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques) ;
- la notification à la CNPD par le fournisseur de services de communications électroniques accessibles au public en cas de violation de données à caractère personnel (article 3 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques) ;
- la communication au GOVCERT des incidents informatiques affectant les systèmes d'information du gouvernement et d'opérateurs d'infrastructures critiques au Luxembourg.



Notons que les administrations ayant recours aux services du CTIE ou ayant, de manière plus générale, accès au réseau de l'Etat, sont tenues de notifier au CTIE tout incident de sécurité détecté.





La présente publication ne prétend pas à l'exhaustivité et n'a pas vocation à couvrir tous les aspects, conditions et exigences de la protection des données et de la sécurité de l'information.
Les informations contenues dans la présente publication ne préjudicient en aucun cas à une interprétation et application des textes légaux par les administrations étatiques et communales ou les juridictions compétentes.
Le CGPD ne peut être tenu responsable pour d'éventuelles erreurs ou omissions dans la présente publication ou de toutes conséquences découlant de l'utilisation des informations contenues dans celle-ci.

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Commissariat du gouvernement
à la protection des données
auprès de l'État

En collaboration avec :

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Haut-Commissariat
à la protection nationale

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

Agence nationale de la sécurité
des systèmes d'information

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

CERT gouvernemental

ctie
Centre des technologies
de l'information de l'État

LHC
Luxembourg House
of Cybersecurity

CNPD
COMMISSION
NATIONALE
POUR LA
PROTECTION
DES DONNÉES

ILR
INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

CCSS
Centre commun de
la sécurité sociale