economie
SPF Economie, P.M.E., Classes moyennes et Energie

Sécurité de l'information
Glossaire

Ce glossaire a été réalisé en rassemblant de nombreuses sources : Larousse, Robert, textes législatifs belges et européens, dictionnaire de l'Agence wallonne des Télécommunications (AWT), du BSI Group, du CERT américain, du SafeOnWeb ainsi que d'autres sources d'informations officielles (Autorité de protection des données, ANSSI,...).

A

Active Directory (AD)	Est une base de données de services annuaires développée par Microsoft et qui offre des mécanismes d'authentification et d'autorisation ainsi qu'un cadre dans lequel d'autres services connexes peuvent être déployés. Via l'AD, il est possible d'authentifier et d'autoriser tous les utilisateurs et ordinateurs d'un réseau de type Windows, en assignant et en appliquant des politiques de sécurité pour tous les ordinateurs et en installant ou en mettant à jour des logiciels.
Adresse IP	Numéro d'identification attribué de façon permanente ou provisoire à chaque appareil connecté à un réseau informatique utilisant le Protocole Internet (IP). Voir IP Internet Protocol
Algorithme	Ensemble de règles opératoires dont l'application permet de résoudre un problème énoncé au moyen d'un nombre fini d'opérations. Un algorithme peut être traduit, grâce à un langage de programmation, en un programme exécutable par un ordinateur.
(App) Application	Une application est un programme (ou software) que vous pouvez installer sur votre ordinateur (PC...), smartphone (GSM) ou tablette. Les applications peuvent être proposées moyennant un prix ou à titre gratuit. Préférez les sites de téléchargement officiels et lisez les conditions générales.

Authentification	Procédure qui consiste, pour un système informatique, à vérifier l'identité d'une personne ou d'un ordinateur afin d'autoriser l'accès de cette entité à des ressources (systèmes, réseaux, applications…)
Autorité de protection des données (APD)	Anciennement Commission de la protection de la vie privée (CPVP). Autorité belge de contrôle des traitements de données à caractère personnel, veillant au respect des règles identifiées par le règlement européen 2016/679 (GDPR). Voir également : Loi du 3 décembre 2017 portant création de l'Autorité de protection des données. Site officiel : https://www.autoriteprotectiondonnees.be/

B

Back door	Ou « porte dérobée ». Il s'agit d'un accès dissimulé, soit logiciel soit matériel, qui permet à un utilisateur malveillant de se connecter à une machine de manière furtive. Une porte dérobée peut notamment permettre au cyberattaquant d'installer un malware, d'accéder à des informations ou d'usurper des droits d'administrateur.
Back-up	Activité qui consiste à copier des fichiers ou des bases de données de manière à les protéger en cas de « catastrophe », notamment d'une défaillance de l'équipement. Pensez à séparer vos back-up de vos fichiers ou bases de données initiales et à faire des tests réguliers sur vos procédures de back-up.
Base de données	Collection de données organisées de façon à être facilement accessibles, administrées et mises à jour. Les bases de données peuvent être classées par le type de contenu qu'elles renferment : bibliographique, full text, images, nombres…

BCP (Business Continuity Plan)	Ensemble de documents, instructions et procédures qui permettent à une entreprise de continuer ses activités en cas d'incident. En lien avec la gestion des incidents. Une partie du BCP peut également prévoir les aspects liés à des catastrophes (voir « DRP »).
Big Data	Des trillions d'octets (bytes) de données sont générés chaque jour et peuvent provenir de toutes sortes de sources : de capteurs utilisés pour collecter des messages sur les sites de médias sociaux, d'images numériques, de vidéos en ligne, d'achats en ligne, de signaux GPS de téléphones mobiles... La gestion de ces larges volumes de données peut causer de grandes préoccupations techniques (stockage, marquage, transfert, visualisation, respect de la vie privée...). Le Big Data entraine de nombreuses questions sur au moins quatre dimensions (4 V) : volume, vélocité, variété et véracité. V pour Volume La quantité phénoménale de données produite chaque jour est en pleine expansion et suit une loi quasi exponentielle. Les réseaux sociaux et le commerce électronique, les fournisseurs d'énergie...sont parmi les grands contributeurs de cette profusion de données. V pour Vélocité (rapidité) Les données sont très rapidement modifiées, mises à jour, remplacées par de nouvelles informations... V pour Variété Les données et bases de données ne suivent pas toutes le même format (texte, image, graphiques...) V pour Valeur Encore faut-il que toutes ces données puisent être exploitées, qu'elle soient « utiles », qu'elles aient une certaine valeur.

Biométrie	Art.4, §14 du GDPR + Considérant 91 « Sont considérées comme des données biométriques, les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques. » Exemple : empreinte digitale, empreinte de l'iris…
Bluetooth	Bluetooth est la norme 802.15.1 permettant des communications radio à courte portée donc sans fil. Il existe plusieurs versions, dont les plus répandues sont actuellement v1.2 (débit théorique de 1 Mbit/s) et v2.0 (débit théorique de 3 Mbit/s).
Botnet	Un botnet est un réseau d'objets connectés (« armée d'appareils zombies ») qui sont utilisés – souvent à l'insu de leurs propriétaires – pour attaquer des sites web ou des serveurs d'entreprises et d'organisations en bombardant les victimes de requêtes (voir DDoS) ou de malwares. N'importe quel objet connecté à internet peut faire partie d'un botnet. Le processus est le suivant : un programme malveillant contamine votre ordinateur mais reste invisible sur celui-ci. Il attend un ordre des cybercriminels. A partir du moment où les cybercriminels ont contaminé suffisamment d'ordinateurs, ils donnent l'ordre aux objets infectés de bombarder un site web ou un serveur déterminé. Dans la plupart des cas, vous ne remarquerez même pas que votre ordinateur est/a été utilisé pour mener une cyberattaque. Des botnets peuvent aussi être loués à d'autres cybercriminels en passant sur le Dark web.
Browser (ou système de navigation)	Un browser ou système de navigation sur internet est un software conçu pour permettre de faire des recherches sur internet et de consulter les pages internet. Les plus connus sont Google Chrome, Mozilla, Safari, internet explorer…

BSI Group

BSI Group est un groupe institutionnel britannique d'organismes de services en normalisation, certification, formation et contrôle de conformité.

BYOD

Bring Your Own Device (parfois rebaptisé « Bring Your Own Disaster »). Les employés utilisent leur propre ordinateur, leurs propres clefs USB, leurs propres GSM à des fins professionnelles.

C

Caméras de surveillance

Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, art. 2

« : tout système d'observation fixe , fixe temporaire ou mobile dont le but est la surveillance et le contrôle des lieux, et qui, à cet effet, traite des images;

4° /1 caméra de surveillance mobile : caméra de surveillance déplacée au cours de l'observation afin de filmer à partir de différents lieux ou positions;

4° /2 caméra de surveillance fixe temporaire : caméra de surveillance fixée pour un temps limité dans un lieu dans l'objectif soit de surveiller un événement déterminé soit d'être déplacée à intervalles réguliers pour être fixée à un autre endroit suivant les finalités qui lui ont été assignées;

4° /3 caméra de surveillance intelligente : caméra de surveillance qui comprend également des composantes ainsi que des logiciels qui, couplés ou non à des registres ou à des fichiers, peuvent traiter de manière autonome ou non les images recueillies ».

Cheval de Troie (Trojans)

Programme informatique (ou malware) qui apparait comme ayant une fonction utile mais qui comporte une/des fonction(s) cachée(s) malintentionnée(s).

Clauses contractuelles types	Il s'agit de modèles d'éléments de contrat qui ont été établis par la Commission européenne ou par l'autorité de contrôle nationale. Ces modèles de clauses ont pour but de faciliter la tâche des responsables du traitement dans la mise en œuvre de contrats et peuvent notamment viser les transferts de données personnelles hors de l'Union européenne ou les relations entre responsable du traitement et sous-traitant (voir notamment art. 46 et 28 GDPR). .
Cloud (Cloud Computing)	« Nuage » (« Informatique en nuage ») Art. 4, § 19 de la directive NIS « un service numérique qui permet l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées. » Technologie qui permet de mettre sur des serveurs localisés à distance des données de stockage ou des logiciels qui sont habituellement stockés sur l'ordinateur d'un utilisateur, voire sur des serveurs installés en réseau local au sein d'une entreprise. Il existe différents types de cloud offrant des degrés de sécurité différents : du cloud public au cloud privé en passant par le cloud hybride. Les services « cloud » peuvent différer : depuis l'infrastructure (IaaS) jusqu'au software (SaaS) en passant par la plateforme (Paas).
COBIT	« Control Objectives for Information and related Technology », en français « Objectifs de contrôle de l'Information et des Technologies Associées » Outil fédérateur permettant d'intégrer de bonnes pratiques, offrant un vocabulaire commun et compatible avec d'autres standards tels que la famille des normes ISO, ITIL, etc.

Comité européen de protection des données	Anciennement « G 29 » (WP29 http://ec.europa.eu/newsroom/article29/news-overview.cfm). Le Comité européen est composé du chef d'une autorité de contrôle de chaque Etat membre et du Contrôleur européen de la protection des données, ou de leurs représentants respectifs. Ce comité publie des lignes directrices, des recommandations et des bonnes pratiques concernant la mise en œuvre du GDPR. Site web officiel : https://edpb.europa.eu/
Command & Control (C&C)	Command & Control (C&C) Moyen par le biais duquel les cyber-attaquants communiquent avec les botnets qu'ils ont infectés. Les serveurs C&C leur permettent de lancer des ordres et de recevoir des informations des botnets qu'ils contrôlent. Voir également « Botnet » et « DDoS ».
Compte administrateur (compte privilégié)	Un compte administrateur (ou privilégié) est un compte bénéficiant de droits d'accès étendus. Ce type de compte est traditionnellement celui des équipes techniques auxquelles vous avez confié la protection de votre réseau. Ces comptes administrateurs font partie des cibles privilégiées des cyberattaquants car elles permettent à des utilisateurs malveillants de porter plus facilement et/ou plus gravement atteinte à la sécurité ou au fonctionnement de votre système d'information (en ce compris les applications métier).
Consentement de la personne concernée	Art. 4, §11 du GDPR et art. 6, 7 et 83, §5, a + considérants 32, 33, 38, 42 et 43 « Toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement. » Attention : la personne concernée peut, dans bien des cas, retirer son consentement.

CPVP	Commission de la protection de la vie privée. Remplacée par l'Autorité de protection des données depuis le 25 mai 2018.
Cryptage/chiffrement	Voir cryptographie.
Cryptographie	Art.2, §40 de la LCE « L'ensemble des services mettant en œuvre les principes, moyens et méthodes de transformation de données dans le but de cacher leur contenu sémantique, d'établir leur authenticité, d'empêcher que leur modification passe inaperçue, de prévenir leur répudiation et d'empêcher leur utilisation non autorisée. » Du grec κρυπτός (cruptos) qui signifie « caché, dissimulé » et γράφειν (graphein) qui signifie « écrire », le chiffrement consiste à transformer une donnée (texte, message ...) en utilisant une « clef » afin de rendre la donnée incompréhensible par toute personne autre que celle à qui est destiné le message. La fonction permettant de retrouver le texte clair à partir du texte chiffré porte le nom de déchiffrement.
Cyber	Terme générique qui désigne, au sens large, tout ce qui est de l'ordre du virtuel ou du multimédia. Traditionnellement, les opportunités offertes par le web sont appelées « digitales » ou « numériques » (économie numérique, agenda digital, Digital single market...) et les risques sont qualifiés de « cyber » (cybersécurité, cyber-risques, cybercriminalité...).
Cyber Squatting	Le cyber squatting (également connu sous le nom de « domaine squatting ») est l'enregistrement, le trafic ou l'utilisation d'un nom de domaine internet de mauvaise foi afin de profiter de la bonne image d'une marque ou du nom commercial d'une autre entreprise.

D

Dark web	Le web (réseau) peut être subdivisé en deux grands groupes : a) Surface web : ce qui est accessible via des browsers (moteurs de recherche) traditionnels comme Google par exemple. b) Deep web : ce qui n'est pas facilement accessible via des browsers traditionnels. Le Dark web est une petite partie du Deep web qui a intentionnellement recours à certaines techniques afin de garantir l'anonymat de ses utilisateurs comme de ses propriétaires. Le Dark web est le plus souvent connu dans les sociétés démocratiques pour être le lieu de nombreuses activités illicites. Le plus connu des browsers permettant aux utilisateurs de naviguer dans le Dark web est TOR (The Onion Router).
Data breach	Voir « violation de données à caractère personnel ».
Data mining	Regroupe l'ensemble des technologies susceptibles d'analyser les informations d'une base de données pour y trouver des informations utiles à l'action marketing et d'éventuelles corrélations signifiantes et utilisables entre les données.
Datawarehouse	Entrepôt de données ou base de données décisionnelles. Base de données utilisée pour collecter, ordonner, journaliser et stocker des informations provenant de bases de données opérationnelles et fournir ainsi un socle à l'aide à la décision en entreprise.

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

DDoS	Distributed Denial of Service ou attaque par déni de service. Une attaque DDoS est une attaque menée contre un serveur ayant pour objectif de l'empêcher de continuer à fonctionner et de rendre l'accès aux utilisateurs légitimes impossible. Un grand nombre d'objets connectés (« botnet ») participent à cette attaque. En raison de la quantité gigantesque d'informations simultanées que le serveur attaqué doit soudain gérer, le serveur ne peut plus traiter les innombrables requêtes et n'est dès lors plus accessible.
Destinataire	Art 4, §9 du GDPR + Considérant 31 « La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un Etat membre ne sont pas considérées comme des destinataires ; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement. »
Directive NIS	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.
Directive 2002/58	Prochainement remplacée par le ePrivacy Regulation Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)

Directive 95/46	Remplacée par le GDPR (25 mai 2018) Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
Domain Name System (DNS)	Art. 4, § 14 de la directive NIS *« Système hiérarchique et distribué d'affectation de noms dans un réseau qui résout les questions liées aux noms de domaines »* Système essentiel au fonctionnement d'internet qui permet d'établir la correspondance entre le nom de domaine et une adresse IP. Par exemple, le DNS établit la correspondance entre le domaine du site web du SPF Economie et notre adresse IP. Grâce au DNS, vous n'êtes pas obligé de connaître notre adresse IP pour nous retrouver.
Donnée à caractère personnel	Art. 4, §1 du GDPR + Considérants 26 à 29 et 38 « Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. »
Donnée perçue comme sensible	Bien que n'étant pas définies comme une catégorie particulière (donnée sensible) de données au sens de l'article 9 GDPR, certaines données sont perçues comme sensibles par les personnes concernées. Il s'agit par exemple de leurs données bancaires.

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

Donnée sensible (catégorie particulière)	Art. 4, 6, 9, 36, 83, §5,a et 89 du GDPR + Considérants 51 à 56 En principe, est interdit le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique (voir art. 9 GDPR).
DPIA	Art. 35 et 83, §4, a du GDPR + Considérants 75, 84, 89 à 93 Data Protection Impact Analysis ou Analyse d'impact relative à la protection des données « Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires. »
Droit à l'information	Art. 12 à 14 du GDPR + Considérants 58 à 62 « Le principe de traitement loyal et transparent exige que la personne concernée soit informée de l'existence de l'opération de traitement et de ses finalités. Le responsable du traitement devrait fournir à la personne concernée toute autre information nécessaire pour garantir un traitement équitable et transparent, compte tenu des circonstances particulières et du contexte dans lesquels les données à caractère personnel sont traitées. La personne concernée dispose d'un droit (non absolu) d'accès à l'information laquelle doit lui être fournie de façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples. »

Droit à l'oubli (Droit à l'effacement)	Art. 6, 8, 9, 12,15, 17, 19, 21, 83, §5, b, 89 du GDPR + considérants 65 et 66 Moyennant le respect de certaines conditions, la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais (voir article 17 GDPR).
Droit d'accès	Art. 15, 30, 83, §5, b du GDPR + considérants 63 et 64 La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel ainsi qu'à certaines informations (voir article 15 GDPR).
Droit d'opposition	Art. 5, art. 6, §1, e) et f), art. 12; art. 21, art. 83, §5, b du GDPR + considérants 69 et 70 La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé sur l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ou aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant, y compris un profilage fondé sur ces dispositions. Le responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice.

Droit de rectification	Art. 5, 12, 19 et Art. 16, art. 83, §5, b du GDPR, + considérants 65 La personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes. Compte tenu des finalités du traitement, la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire.
Dropper	Software parasite (type cheval de Troie) chargé d'introduire, décompresser et installer un autre software malicieux.
Drown attack	Les attaques de type « Drown » permettent à des cyberattaquants de capturer des informations entre un utilisateur et un site web « https ». La mention « https » assure, a priori, qu'il s'agit d'un site sécurisé. Toutefois, les attaques drown exploitent des failles des serveurs qui supportent des technologies obsolètes de type SSLv2 (prédécesseurs de TLS). Pour lutter contre ce type d'attaque, il convient d'user d'une clef de cryptographie récente. Aucun serveur TLS ne devrait user d'une version SSL. Pour plus d'information, voir : https://drownattack.com/ https://www.enisa.europa.eu/publications/info-notes/the-drown-attack
DRP (Disaster Recovery Plan)	Un Disaster Recovery Plan, parfois aussi appelé Plan de reprise d'activité (PRA), permet de reprendre rapidement une activité après une catastrophe (inondation, incendie, coupure de courant non planifiée…) au moins pour ce qui concerne les missions critiques de l'entreprise. Le DRP identifie quelles activités doivent être reprises en premier, définit le rôle de chacun des employés et offre les procédures à suivre. Voir également « BCP ».

E

EBIOS	La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) est un outil français (ANSSI). L'EBIOS permet une gestion des risques de sécurité des systèmes d'information assez complète et correspond à des standards internationaux tels que ISO/IEC 27001, ISO/IEC 27005 et ISO/IEC 31000.
ECSO (European Cyber Security Organisation)	Association sans but lucratif représentant les intérêts du secteur privé, du secteur académique et du secteur public auprès de la Commission européenne en matière de cybersécurité. L'ECSO soutient les initiatives et projets européens permettant de développer, d'encourager et de promouvoir la cybersécurité en Europe. Divisée en plusieurs groupes de travail, elle offre à différents secteurs et entreprises la possibilité de faire valoir leurs points de vue et de partager de l'information.
e-government (e-Gov)	Consiste à rendre électroniques tout ou partie des services rendus par les administrations aux citoyens, aux entreprises, aux autres administrations, etc. Par exemple, l'application tax-on-web en Belgique permet au citoyen de remplir via internet sa déclaration d'impôt sur le revenu.
e-health	Plate-forme belge des technologies de l'information et de la communication appliquées à la santé.
Encryption	Voir cryptographie.
ePrivacy Regulation	Futur règlement européen remplaçant la directive 2002/58, protégeant la vie privée dans le cadre des communications électroniques.

ERP (Entreprise Ressource Planning)	Parfois appelés « PGI » (progiciel de gestion intégré). L'ERP est un système intégré qui optimise les processus de gestion d'une entreprise en fédérant toutes les applications, de la comptabilité à la gestion des ressources humaines, en passant par le management de projets et la logistique. Les ressources sont partagées et les différents services de l'entreprise ont accès aux bases de données actualisées en temps réel. Les plus connus sont notamment SAP, Oracle, Sage, Microsoft Business Solutions, Generix...

F

Fichier	Art. 4, § 6 du GDPR Tout ensemble structuré de données à caractère personnel accessible selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.
Finalités d'un traitement	Objectifs poursuivis par un/des ensemble(s) d'opérations sur des données. Les finalités d'un traitement de données à caractère personnel doivent répondre aux critères prévus par l'article 5, §1, b GDPR.
Firewall	En français « pare-feu », outil permettant de limiter le trafic sur le web entre le réseau et le système d'information. Un hardware/software qui permet de limiter le trafic réseau sur la base d'un ensemble de règles fixées au préalable et déterminant quels accès sont autorisés. Voir également « WAF »
Forensic(s)	Application de techniques et méthodes scientifiques concernant des infractions et crimes. En matière cyber, il s'agit de pouvoir conserver et analyser les preuves relatives à des cyberattaques. Ces méthodes sont appliquées aussi bien par les autorités (FCCU, CERT...) que par les entreprises afin de pouvoir identifier les cyberattaquants mais également afin de lutter plus efficacement contre les cyberattaques en apprenant des leçons de celles-ci.

G

G29 (groupe article 29) (WP29)

Ancien nom du Comité européen de protection des données (voir l'article 29 de la directive 95/46).

GDPR (également connu sous le nom français RGPD)

General Data Protection Regulation
Règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

Géolocalisation

La géolocalisation regroupe un ensemble de procédés techniques par lesquels il est possible de localiser géographiquement, le plus souvent en temps réel, des individus. Les techniques de géolocalisation ont d'abord été utilisées pour géolocaliser les utilisateurs d'internet sur ordinateur (géolocalisation IP) avant que les usages explosent par le biais des capacités de géolocalisation associés à l'usage des mobiles et des applications.

H – I

Hardware

Le hardware qualifie le matériel informatique en général, par opposition au software, qui désigne les programmes et logiciels.

Https

Hypertext Transfer Protocol Secure.
Ce sigle en haut à gauche de la barre de recherches signifie que la connexion est en principe sécurisée.

(IaaS) Infrastructure as a Service

Forme de cloud qui permet à l'entreprise d'obtenir de son fournisseur cloud des ressources matérielles abstraites (typiquement des machines virtuelles) et de disposer à tout moment de la puissance de calcul, de l'espace de stockage et de la vitesse de communication dont elle a besoin.

(IAM) Identity and Access Management	Gestion des identités et des accès. L'IAM est une discipline de sécurité qui permet de gérer de manière centrale la liste des utilisateurs ainsi que d'identifier leurs droits d'accès.
IBPT	Institut Belge des services Postaux et des Télécommunications, notamment chargé de la régulation des services relatifs aux télécommunications et à l'internet en Belgique.
Incident	Art. 4 de la directive NIS « Tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information. » Un Incident Management Plan est un plan de gestion des incidents.
Indicateurs de compromission (IoC)	Les indicateurs de compromission sont l'un des outils qui permettent de détecter de manière (quasi) automatique la présence d'une menace portée sur le système d'information. A eux seuls, les IoC ne peuvent suffire à détecter un incident ou un problème mais ils constituent néanmoins une première ligne de détection.
Infrastructure critique	Art. 3 de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques « installation, système ou partie de celui- ci, d'intérêt fédéral, qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'interruption du fonctionnement ou la destruction aurait une incidence significative du fait de la défaillance de ces fonctions. »
Insider Threat	Une personne physique ou un groupe de personnes physiques au sein d'une organisation qui pose un risque en violant les règles de sécurité de manière intentionnelle ou non.

Intrusion Detection System (IDS)	Un IDS est un système de détection d'intrusion qui surveille les activités suspectes sur le réseau. L'IDS avertit les administrateurs mais ne bloque pas les attaques (voir IPS). Certains IDS peuvent être configurés pour détecter les violations de votre politique de sécurité.
IoT (Internet of Things)	Caractérise des objets physiques connectés ayant leur propre identité numérique et capables de communiquer les uns avec les autres. Ce réseau crée en quelque sorte une passerelle entre le monde physique et le monde virtuel. Une montre connectée, des lunettes connectées, des caméras connectées, des compteurs intelligents sont autant d'exemples d'IoT.
IP Internet Protocol	La communication via internet est fondée sur un protocole qui permet aux ordinateurs de communiquer entre eux. Ce protocole est appelé IP pour Internet Protocol. Chaque machine connectée est distinguée des autres par une adresse numérique. La communication entre machines se fait par envoi de paquets d'informations contenant chacun une adresse de source et une adresse de destination. Il existe plusieurs versions (v) de protocole IP. Actuellement, l'IPv6 est en cours de déploiement (8 nombres notés en hexadécimal) même s'il reste de nombreuses machines connectées via IPv4. L'IPsec désigne un protocole de chiffrement et de signature des paquets IP.
IPS Intrusion Prevention System	Un IPS est un système assurant le contrôle du trafic réseau qui permet, en cas d'attaque, d'analyser des données concernant la menace et de prendre les mesures correctrices nécessaires (par exemple en imposant certaines règles au firewall de l'entreprise).

ISP Internet Service Provider	Appelés également fournisseurs d'accès à internet ou « FAI ». Un ISP (ou FAI) propose des services de connexion au web ainsi que des services complémentaires éventuels (adresse e-mail…)
ITIL	Information Technology Infrastructure Library (ITIL). Référentiel présentant une collection de bonnes pratiques pour assurer un management efficace du système d'information.
IXP (Point d'échange internet)	Art. 4, § 13 de la directive NIS « Une structure de réseau qui permet l'interconnexion de plus de deux systèmes autonomes indépendants, essentiellement aux fins de faciliter l'échange de trafic internet ; un IXP n'assure l'interconnexion que pour des systèmes autonomes ; un IXP n'exige pas que le trafic internet passant entre une paire quelconque de systèmes autonomes participants transite par un système autonome tiers, pas plus qu'il ne modifie ou n'altère par ailleurs un tel trafic. »

J – K – L

Key logger	Software ou hardware qui traque les mouvements (ta-blettes) ou les frappes sur les touches de manière dis-crète afin de récupérer des informations (connaissance des fichiers, mots de passe, codes secrets…).
LCE	Loi du 13 juin 2005 relative aux communications électroniques.
LDPA	LDAP (Lightweight Directory Access Protocol) est un protocole d'application pour interroger et modifier des éléments dans les bases de données de services d'annuaire comme Active Directory (AD).
Licéité d'un traitement	Voir traitement licite.

Limitation de traitement	Art 4, §3 et art. 18 du GDPR + considérant 67 « Le marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur. »
Logiciel	Voir software
Logiciel libre	Software donné ou vendu avec son code source accompagné d'une licence dont les termes permettent légalement la copie, la revente et la diffusion sans frais supplémentaire par l'acheteur initial. Cette licence interdit, en principe, que des intérêts privés utilisent et modifient un logiciel libre et en fassent un produit propriétaire.
LVP	Ancienne Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (transposant l'ancienne directive 95/46). Voir « GDPR ».

M – N – O

Malwares	Programmes logiciels (softwares) malicieux. Software qui compromet le bon fonctionnement d'un système d'information en exécutant une fonction ou un processus non autorisé. Voir également « ransomwares » et « chevaux de Troie ».
Matrice d'escalade	Une matrice d'escalade est un plan et/ou une procédure mise en place pour faire face à des problèmes potentiels dans divers contextes. La matrice d'escalade identifie qui doit être contacté en fonction de la gravité (impact) de l'incident ou du problème identifié et des capacités opérationnelles et/ou décisionnelles (stratégiques) requises pour résoudre le problème et/ou maîtriser la communication vers l'extérieur.
MEHARI	MEHARI (MEthod for Harmonized Analysis of RIsk) est une méthode gratuite (open source) d'analyse de risques et de gestion des risques s'alignant avec les normes ISO/IEC 27001:2013 et ISO/IEC 27005 :2011

Métadonnées	Ensemble structuré d'informations servant à décrire une ressource. Pour prendre un exemple, dans le cas d'un mail, les métadonnées qu'il serait pertinent de lui associer seraient le nom de l'expéditeur, le nom du destinataire, l'heure à laquelle le mail a été envoyé… par opposition à la donnée elle-même qui, pour reprendre cet exemple, serait le contenu de l'e- mail, le message en lui-même.
Mitiger (mitigation)	Mitiger les risques : appliquer une ou plusieurs mesures afin de réduire la probabilité d'une menace et/ou d'en réduire les conséquences (par exemple en transférant une partie de ce risque).
MONARC	Monarc est une méthode gratuite et optimisée d'analyse de risques d'origine luxembourgeoise. Cette méthode permet d'établir un rapport complet des risques en la matière et d'identifier des pistes de solutions.
NIS	Security of Network and Information Systems Abréviation anglaise désignant la directive 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'informations dans l'Union.
NIST	National Institute of Standards and Technology (U.S Department of Commerce).
Open Data	Données considérées comme pouvant être accessibles à tous sans protection particulière (droit d'auteur) ni mécanismes de contrôle préalables. Sont par exemple « open data » les statistiques sur l'emploi (data.gov.be).

Opérateur de service essentiel (OSE)	Art. 4, §4 de la directive NIS (voir également art. 5, §2 et annexe II de la directive NIS) Entité publique ou privée dans les secteurs de l'Energie, du Transport, des Banques, des infrastructures de marchés financiers, des établissements de soins de santé, de fourniture et distribution d'eau potable et d'infrastructures numériques et qui répond aux critères suivants : a) une entité fournit un service qui est essentiel au maintien d'activités sociétales et/ou économiques critiques ; b) la fourniture de ce service est tributaire des réseaux et des systèmes d'information ; et c) un incident aurait un effet disruptif important sur la fourniture dudit service. Les opérateurs de service essentiels couvrent les infrastructures critiques dans les secteurs prédéfinis ainsi que d'autres entités pourvu qu'elles répondent aux critères précités. Voir également « infrastructure critique ».
Operating System (OS)	Un operating system (OS) ou « système d'exploitation » est un programme permettant à l'ensemble des applications de fonctionner et facilitant la manipulation des programmes pour l'utilisateur.
Opt In/Opt Out	Les termes opt in/opt out réfèrent à diverses méthodes par lesquelles des personnes concernées peuvent refuser un traitement de leurs données à caractère personnel. L'opt in implique que la personne concernée doit manifester son consentement au préalable alors que l'opt out implique que le traitement a lieu par défaut et que la personne concernée doit manifester sa volonté d'y mettre un terme en adoptant une démarche active. Une liste telle que « bel-me-niet-meer » est une liste de type « opt out » permettant aux personnes ayant fait la démarche de s'y inscrire de ne plus recevoir de coup de téléphone non sollicité à caractère commercial.

P

PaaS (Platform as a Service)	Forme de cloud qui permet à l'entreprise d'obtenir de son fournisseur cloud un accès à une plateforme de développement. Il s'agit d'un environnement spécifique dans lequel l'entreprise peut concevoir et tester des applications qui tournent sur cette plateforme ou sur une installation similaire. La plateforme (middleware) définit les standards qui permettront de s'adresser de manière large et interopérable à de nombreux clients et d'élargir leur choix en matière de logiciels.
Patch	Un patch comprend un ensemble de modifications apportées à un programme logiciel et sert notamment à tenir à jour le logiciel concerné, à corriger certaines failles ou à améliorer certains critères (performance, maniabilité..).
Personne concernée	Art. 4, §1 du GDPR, + considérants 26 à 29 et 38 « Une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. »
Phishing	Forme d'ingéniérie sociale numérique (e-mails) ayant pour but de soutirer des informations clefs à des individus (mots de passe, numéros de comptes bancaires, comptabilité de l'entreprise...).
PNR	Passenger Name Record Loi du 25 décembre 2016 relative au traitement des données des passagers.

Prince2	Méthode de management de projet orientée processus.
Principe de proportionnalité	Le principe de proportionnalité implique que l'on ne peut collecter que les données à caractère personnel qui sont « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement ». Cela suppose que seules les données pertinentes et nécessaires peuvent être collectées.
Privacy Policy	Une « privacy policy » ou « politique de confidentialité des données (à caractère personnel) » est un document à caractère juridique qui apporte quelques précisions sur la façon dont le responsable du traitement recueille, utilise, divulgue et gère les données d'une personne concernée (client). La privacy policy permet notamment de répondre à une obligation légale de transparence qui pèse sur le responsable du traitement.
Privileged Identity Management (PIM)	Système de gestion de comptes privilégiés (IT administrateurs...).
Profilage	Art. 4, §4 du GDPR + considérants 30 et 91 « Toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique. »

Proxy

Un « proxy » est un système dédié ou un logiciel fonctionnant sur un ordinateur et qui sert d'intermédiaire entre un dispositif terminal (par exemple, un ordinateur), et un autre serveur sur lequel un utilisateur ou un client demande un service. Un proxy peut notamment permettre de surfer de manière « anonyme » sur internet.

Pseudonimisation

Art.4, §5 du GDPR + considérants 26, 28, 29
« Le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable ».

PUP

Potentially Unwanted Programs
Software potentiellement indésirable souvent associé à des applications « à titre gratuit » et qui peut faire apparaitre des fenêtres « pop-up » (adware), installer des modifications dans la barre d'outils du browser, modifier la page d'accueil et/ou exécuter des processus en tâches de fond qui peuvent ralentir les performances du système d'information.

Q – R

Ransomware

Un ransomware est un software malveillant (malware) qui encrypte les données figurant sur l'appareil infecté tout en promettant de restituer les données moyennant paiement d'une rançon (en bitcoins).
Voir https://www.nomoreransom.org/ et https://ransomfree.cybereason.com/

Recovery (ou restauration)	Il peut s'agir d'un point de sauvegarde permettant, en cas de défaillance du système d'information, de revenir à un état antérieur à la défaillance (point de restauration) ou d'un plan comme le Disaster Recovery Plan qui prévoit comment assurer les missions critiques en cas de désastre (catastrophe).
Règlement général sur la protection des données (RGPD)	Voir GDPR.
Responsable de traitement	Art.4, §7 du GDPR + articles 24 à 43 « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un Etat membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un Etat membre. »
RFID (Radio Frequency IDentification)	Méthode utilisée pour stocker et récupérer des données à distance en utilisant des balises métalliques qui peuvent être collées ou incorporées dans des produits.
Risques	Toute circonstance ou tout événement raisonnablement identifiable ayant un impact négatif potentiel sur la sécurité des réseaux et des systèmes d'information.

S

SaaS (Software as a Service)	Forme de cloud qui permet à l'entreprise d'acheter une application complète et opérationnelle à laquelle l'utilisateur accède au moyen de son navigateur Web ou d'un autre logiciel client. Cette solution diminue le nombre d'installations de software sur chaque appareil du client, voire les rend inutiles.

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

Secret professionnel	Art. 458 du Code pénal « Les médecins, chirurgiens, officiers de santé, pharmaciens, sages-femmes et toutes autres personnes dépositaires, par état ou par profession, des secrets qu'on leur confie, qui, hors le cas où ils sont appelés à rendre témoignage en justice (ou devant une commission d'enquête parlementaire) et celui où la loi les oblige à faire connaître ces secrets, les auront révélés, seront punis d'un emprisonnement de huit jours à six mois et d'une amende de cent euros à cinq cents euros. » (NB : à multiplier par les décimes additionnels. NLDR : les amendes à dater du 1er janvier 2017 sont multipliées par 8).
Sécurité des systèmes et des réseaux	La capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles.
SIEM	Security Information and Event management Les outils SIEM permettent d'agréger des informations sur le réseau, de les trier et de les comparer (corréler) afin de détecter des activités suspicieuses en monitorant des applications, des comportements utilisateurs et des accès aux données. Ne vous reposez pas uniquement sur eux et n'oubliez pas que la qualité des règles de détection et de corrélation, la couverture des types d'incidents et les processus de réponse en cas de détection doivent également être implémentés de manière efficace.
SLA (Service Level Agreement)	Le SLA est un contrat, ou une partie du contrat fixant les niveaux de service attendus en associant à chaque niveau de service des sanctions possibles.

	Le SLA identifie les besoins (principaux) du bénéficiaire, fournit un cadre général de compréhension pour les deux parties, fixe des éléments objectifs en limitant les attentes irréalistes et peut transformer une obligation de moyen en obligation de résultat. Un SLA peut également être utilisé comme outil de marketing par les services commerciaux d'une entreprise envers ses bénéficiaires.
SLM	Le Service Level Manager (SLM) est un gestionnaire qui identifie les niveaux de service attendus en interne/à offrir en externe et qui veille à ce que ces niveaux soient respectés. Le Service Level Manager collabore avec les services internes/externes afin que tous les processus de gestion des services informatiques qui permettent d'assurer ces niveaux de service soient respectés.
Smart grids	« Grille intelligente » permettant aux détenteurs de réseaux énergétiques de contrôler les flux d'énergie et d'ajuster leurs prix en fonction de l'offre et de la demande. Couplé avec du smart metering, le smart grid peut s'appliquer au consommateur en lui fournissant des informations relatives à sa consommation, et en lui permettant d'ajuster ses dépenses en temps réel .
Software	Ensemble de programmes et de procédures nécessaires au fonctionnement d'un système informatique (par opposition à Hardware). Voir également « application ». Lorsqu'ils sont malicieux, les softwares sont appelés « malwares » (voir également « malwares »).
Sous-traitant	Art.4, §8 et art. 28 du GDPR + Considérant 81 « La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. »

Sybil attack	Il s'agit d'atteindre à la réputation en ligne d'un fournisseur de biens ou de services. Dans le cas d'une attaque « Sybil », l'attaquant crée de multiples identités ou profils et use de ses multiples comptes pour manipuler les scores de réputation d'une entreprise ou d'un service en ligne. La réputation d'un site peut ainsi être artificiellement gonflée ou, au contraire, endommagée sans qu'il y ait de rapport concret avec la réalité.
Système d'exploitation	Voir « operating system (OS) »

T

Tiers	Art.4, §10 du GDPR « Une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel. »
(TLP) Traffic Light Protocol	Sorte de classification, de catégorisation des données qui a recours à un code couleur (généralement 4 couleurs : rouge, ambre, vert et blanc) afin de s'assurer que les informations sensibles ne sont partagées qu'avec les personnes adéquates.
Traitement (de données à caractère personnel)	Art. 4, §2 du GDPR « 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, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction. »

Traitement licite	Art. 5, 6, 83, §5, a du GDPR + Considérants 40 à 50 Le traitement de données à caractère personnel doit respecter les conditions prévues à l'article 5 du GDPR. Parmi ces conditions figure la licéité du traitement (voir article 6 du GDPR).
Transfert de données (à caractère personnel)	Art. 44 à 50 du GDPR + Considérants 101 à 116 Un transfert, vers un pays tiers ou à une organisation internationale, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu que moyennant certaines conditions (voir articles 44 à 50 du GDPR).
Transparence	Art. 5, art. 12 à 14 et 15 à 22, art. 34 du GDPR + Considérants 58 et 59 Le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 du GDPR ainsi que pour procéder à toute communication au titre des articles 15 à 22 du GDPR et de l'article 34 du GDPR en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant. Les informations sont fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique. Lorsque la personne concernée en fait la demande, les informations peuvent être fournies oralement, à condition que l'identité de la personne concernée soit démontrée par d'autres moyens.

U – V – W – X – Y – Z

URL	Uniform Resource Locator (localisateur uniforme de ressources). Moyen par lequel une information est retrouvée sur le web (WWW).

Vidéosurveillance/ vidéoprotection	Voir caméras de surveillance.
Violation de données à caractère personnel	Art. 4, §12 ; 33 et 34 du GDPR +considérants 73 et 85 une violation de la sécurité ou « data breach » 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.
VPN	Virtual Private Network Le VPN permet d'établir une connexion sécurisée en chiffrant les communications entre votre ordinateur et le serveur de votre entreprise. Exemple : vous bénéficiez d'une connexion wi-fi peu sécurisée (wi-fi public d'un hôtel, d'une gare...) et vous souhaitez envoyer et/ou recevoir des données professionnelles de votre entreprise. Si vous passez par un VPN, le router du wi-fi sur lequel vous vous êtes connecté ne verra passer que des données chiffrées, les données de votre entreprise resteront protégées.
WAF	Web Application Firewall En plus de fonctionner comme un pare-feu standard, un WAF peut également permettre de filtrer des contenus, de lutter contre les spam, de détecter des tentatives d'intrusion et de détecter certains virus. Voir également « Firewall ».
Web (WWW)	World Wide Web ou « Web » qui signifie littéralement « Toile dans le monde entier» et sert à désigner « Internet ».
Wi-fi	Connexion Internet sans fil
Zombie	Voir Botnet.