economie
FOD Economie, K.M.O., Middenstand en Energie

Informatiebeveiliging
Woordenlijst

Deze woordenlijst is gebaseerd op verschillende bronnen: Larousse, Robert, Belgische en Europese wetgeving, lexica van het Agence wallonne des Télécommunications (AWT), BSI Group, het Amerikaanse CERT, SafeOnWeb alsook andere officiële informatiebronnen (Gegevensbeschermingsautoriteit (GBA), ANSSI, ...).

A

Aanbieder van essentiële diensten

Art. 4, §4 NIS-richtlijn (zie ook art. 5, §2 en bijlage II NIS-richtlijn)
Publieke of private entiteit binnen de sectoren Energie, Transport, Bankwezen, financiële marktinfrastructuren, zorginstellingen, levering en distributie van drinkwater en digitale infrastructuur en die voldoet aan de volgende criteria:
a) een entiteit verleent een dienst die van essentieel belang is voor de instandhouding van kritieke maatschappelijke en/of economische activiteiten;
b) de verlening van die dienst is afhankelijk van netwerk- en informatiesystemen; en
c) een incident zou aanzienlijke verstorende effecten hebben voor de verlening van die dienst.

De aanbieders van essentiële diensten zijn belast met de kritieke infrastructuur binnen de vooraf omschreven sectoren alsook van andere entiteiten op voorwaarde dat ze voldoen aan bovengenoemde criteria. Zie ook "kritieke infrastructuur".

Active Directory (AD)

Een database van jaarlijkse diensten ontwikkeld door Microsoft en die authenticatie en autorisatiemiddelen aanbiedt alsook een kader waarbinnen andere verbonden diensten ontwikkeld kunnen worden. D.m.v. AD is het mogelijk om alle gebruikers en computers op een netwerk van het type Windows te authentiseren en autoriseren.

Administratoraccount (bevoorrecht account)	Een administratoraccount (of bevoorrecht account) is een account die over uitgebreide toegangsrechten beschikt. Dit type account is traditioneel voorbehouden voor technisch personeel aan wie u de bescherming van uw netwerk hebt toevertrouwd. Administratoraccounts zijn een voorkeursdoelwit voor cyberaanvallen, aangezien zij aan kwaadaardige gebruikers toelaten om op een eenvoudige en/of op meer ernstige wijze de beveiliging of werking van uw informatiesysteem (werkmiddelen inbegrepen) te beschadigen.
Algoritme	Een set regels om een bepaald probleem op te lossen aan de hand van een eindig aantal bewerkingen. Een algoritme kan, via programmeertaal, worden vertaald in een door een computer uitvoerbaar programma.
Als gevoelig beschouwde gegevens	Ook al worden ze niet gedefinieerd als een bijzondere categorie (gevoelige gegevens) in de zin van artikel 9 GDPR, toch kunnen bepaalde gegevens door betrokken personen als gevoelig worden beschouwd. Het kan dan bijvoorbeeld gaan om hun bankgegevens.
(App) Applicatie	Een applicatie is een programma (of software) om te installeren op computer (pc, ...), smartphone (gsm) of tablet. Er zijn betaalde en gratis applicaties. Maak bij voorkeur gebruik van officiële downloadsites en lees de algemene voorwaarden.
Authenticatie	Proces waarbij een computersysteem de identiteit van een persoon of computer verifieert om deze entiteit toegang te kunnen verlenen tot bepaalde bronnen (systemen, netwerken, applicaties, ...)

B

Back door	Of "achterdeurtje". Het betreft een verborgen toegang, ofwel in de software ofwel in de hardware, waarmee een kwaadwillende gebruiker op heimelijke wijze verbinding kan maken met een machine. Een achterdeur kan de cyberaanvaller in staat stellen om malware te installeren, toegang te krijgen tot informatie of beheerdersrechten op te eisen, ...

Back-up	Activiteit die erin bestaat bestanden of databanken te kopiëren om ze te beschermen in geval van een "catastrofe", voornamelijk bij uitvallen van apparatuur. Denk eraan om uw back-ups gescheiden te houden van uw bestanden of oorspronkelijke databanken en om regelmatig uw back-upprocedures te testen.
BCP (Business Continuity Plan)	Geheel van documenten, instructies en procedures die aan een onderneming toelaten om haar activiteiten ver-der te zetten in geval van crisis. Dit ligt in lijn met het beheer van incidenten. Een deel van het BCP kan ook voorzien in de aspecten gelinkt aan catastrofes (zie "DRP")
Beperken van de verwerking	Art 4, §3 en art. 18 GDPR + overweging 67 "Het markeren van opgeslagen persoonsgegevens met als doel de verwerking ervan in de toekomst te beperken."
Beroepsgeheim	Art. 458 Strafwetboek "Geneesheren, heelkundigen, officieren van gezondheid, apothekers, vroedvrouwen en alle andere personen die uit hoofde van hun staat of beroep kennis dragen van geheimen die hun zijn toevertrouwd, en deze bekendmaken buiten het geval dat zij geroepen worden om in recht of voor een parlementaire onderzoekscommissie getuigenis af te leggen en buiten het geval dat de wet hen verplicht die geheimen bekend te maken, worden gestraft met gevangenisstraf van acht dagen tot zes maanden en met geldboete van honderd euro tot vijfhonderd euro." (NB: te vermenigvuldigen met de zogenaamde 'opdeciemen': geldboetes worden sinds 1 januari 2017 vermenigvuldigd met 8).
Bestand	Art. 4, § 6 GDPR Elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid.

Besturingssysteem	Zie "operating system (OS)"
Betrokkene	Art. 4, §1 GDPR, + overweging 26 tot 29 en 38 "Natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online-identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon."
Beveiliging van netwerk- en informatiesystemen	Het vermogen van netwerk- en informatiesystemen om met een bepaalde mate van betrouwbaarheid bestand te zijn tegen acties die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van de opgeslagen, verzonden of verwerkte gegevens of de daaraan gerelateerde diensten die via die netwerk- en informatiesystemen worden aangeboden of toegankelijk zijn, in gevaar brengen.
Bewakingscamera's	Art. 2 Wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's 4° bewakingscamera: elk vast, tijdelijk vast of mobiel observatiesysteem dat de bewaking en het toezicht van de plaatsen tot doel heeft en dat hiervoor beelden verwerkt 4° /1 mobiele bewakingscamera: bewakingscamera die tijdens de observatie wordt verplaatst om vanaf verschillende plaatsen of posities te filmen; 4° /2 tijdelijke vaste bewakingscamera: bewakingscamera die voor een beperkte tijd op een plaats wordt opgesteld met als doel hetzij een welbepaald evenement te bewaken, hetzij op regelmatige tijdstippen te worden verplaatst om op een andere plaats te worden opgesteld overeenkomstig de doeleinden die eraan werden toegewezen;

4° /3 intelligente bewakingscamera: bewakingscamera die ook onderdelen en software bevat, die al dan niet gekoppeld aan registers of bestanden, de verzamelde beelden al dan niet autonoom kunnen verwerken;

Big Data

Biljoenen octets (bytes) over gegevens worden elke dag gegenereerd en kunnen voortkomen uit alle soorten bronnen: boodschappen op sociale media, digitale afbeeldingen, online video's, online aankopen, GPS-signalen van mobiele telefoons,... Het beheer van deze grote volumes gegevens kan leiden tot grote technische bezorgdheden (opslag, markering, transfer, visualisatie, respect voor de persoonlijke levenssfeer,...).

Big Data kan talrijke vragen naar voor brengen, die minstens betrekking hebben op vier dimensies (4 V): Volume, Velocity, Variety en Veracity.

V van Volume
De enorme hoeveelheid gegevens die dagelijks gegenereerd worden is in volle expansie en volgt een bijna exponentiële wet. De sociale netwerken, de elektronische handel, de leveranciers van energie,... vallen onder de grootste bijdragers in deze overvloed van gegevens.

V van Velocity (snelheid)
De gegevens worden zeer snel gewijzigd, geüpdatet, vervangen door nieuwe informatie,...

V van Variety (verscheidenheid)
De gegevens en databanken volgen niet allen hetzelfde format (tekst, afbeeldingen, grafieken,...)

V van Veracity (waarachtigheid)
De gegevens moeten ook nog geëxploiteerd kunnen worden, ze moeten een zeker "nut" hebben en dus een zekere waarachtigheid/betrouwbaarheid hebben.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Biometrie	Art.4, §14 GDPR + overweging 91 "Worden beschouwd als biometrische gegevens, persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens." Voorbeeld: vingerafdruk, irisscan, ...
BIPT	Belgisch Instituut voor Postdiensten en Telecommunicatie, voornamelijk belast met de regelgeving en de controle op de telecommunicatieoperatoren en de postbedrijven in België.
Bluetooth	Onder de naam Bluetooth zit de standaard 802.15.1 verborgen die radiocommunicatie met een kort bereik mogelijk maakt, dus via een draadloze verbinding. Er bestaan verschillende versies, waarvan de meestverspreide momenteel v1.2 (theoretische snelheid van 1 Mbit/s) en v2.0 (theoretische snelheid van 3 Mbit/s) zijn.
Botnet	Een botnet is een netwerk van geconnecteerde objecten ("een leger van zombieapparaten") die worden gebruikt – vaak zonder dat de eigenaars zich daar bewust van zijn – om websites of servers van bedrijven en organisaties aan te vallen door deze te bestoken met verzoeken (zie DDoS) of malware. Om het even welk object dat verbonden is met internet, kan deel uitmaken van een botnet. Het procedé is als volgt: een kwaadaardig programma besmet uw computer maar blijft onzichtbaar. Het wacht op een opdracht van cybercriminelen. Zodra cybercriminelen voldoende computers hebben besmet, geven ze die geïnfecteerde objecten opdracht om een bepaalde website of server te bestoken. In de meeste gevallen merkt u zelfs niet dat uw computer wordt/is gebruikt voor een cyberaanval. Botnets kunnen ook worden verhuurd aan andere cybercriminelen via het darkweb.

Browser (of navigatiesysteem)	Een browser of internetnavigatiesysteem is software voor het opgeven van zoekopdrachten en consulteren van internetpagina's. De meest bekende zijn Google Chrome, Mozilla, Safari, internet explorer, ...
BSI Group	BSI Group is de Britse nationale instelling voor normalisatie, certificering, opleiding en conformiteitscontrole.
BYOD	Of "Bring Your Own Device" (vaak herdoopt tot "Bring Your Own Disaster"). De medewerkers gebruiken hun eigen computer, eigen USB-stick, eigen gsm,... voor professionele doeleinden.

C

CBPL	Commissie voor de Bescherming van de Persoonlijke Levenssfeer. Vervangen door de Gegevensbeschermingsautoriteit op 25 mei 2018.
Cloud (Cloudcomputing)	"Cloud" (Cloudcomputing) Art. 4, § 19 NIS-richtlijn "een digitale dienst die toegang mogelijk maakt tot een schaalbare en elastische pool van deelbare computercapaciteit." Technologie voor het, via een server, op afstand opslaan van gegevens of software die doorgaans wordt geïnstalleerd op de computer van de gebruiker of zelfs op de servers van het lokale netwerk van een bedrijf. Er bestaan verschillende soorten clouddiensten, elk met een verschillend niveau van veiligheid: de public cloud, de private cloud en de hybrid cloud. Clouddiensten kunnen verschillen op gebied van infrastructuur (IaaS), platform (Paas) en software (SaaS).
COBIT	"Control Objectives for Information and related Technology" Verbindende tool om goede praktijken te integreren, gebaseerd op een gemeenschappelijke communicatietaal en in overeenstemming met andere normen zoals ISO, ITIL, enzovoort.

Command & Control (C&C)

Middel waarvan cyberaanvallers gebruikmaken om te communiceren met de door hen besmette botnets. Met de C&C-servers kunnen ze commando's doorgeven en informatie ontvangen van de botnets waarover ze controle hebben.
Zie ook "Botnet" en "DDoS".

Cyber

Algemene term die in ruime zin verwijst naar alles wat te maken heeft met virtuele realiteit en multimedia.

Doorgaans worden de door het web geboden mogelijkheden "digitaal" genoemd (digitale economie, digitale agenda, Digital Single Market, ...) en worden de risico's als "cyber" aangeduid (cyberveiligheid, cyberrisico's, cybercriminaliteit, ...).

Cyber Squatting

Cyber Squatting (ook gekend onder de naam "domain squatting" of "domeinkaping") is de registratie, het verkeer of het onrechtmatig gebruik van een domeinnaam op het internet om zo te kunnen profiteren van het goede imago van een commercieel merk of naam van een andere onderneming.

D

Darkweb

Het web (internet) kan in twee hoofdgroepen worden onderverdeeld:

a) Surfaceweb: toegankelijk via traditionele browsers en zoekmachines zoals Google.

b) Deepweb: niet gemakkelijk toegankelijk via traditionele browsers.

Het darkweb is een klein onderdeel van het deepweb waar bewust technieken worden aangewend om anonimiteit van verzenders en ontvangers te garanderen. Het darkweb staat, binnen democratische samenlevingen, vaak bekend als de plek waar zich veel illegale activiteiten afspelen. De meest bekende browser om anoniem te surfen binnen het darkweb is TOR (The Onion Router).

Databank	Verzameling van gegevens georganiseerd op een manier waarop deze makkelijk toegankelijk zijn, gebruikt en geüpdatet kunnen worden. Databanken kunnen geklasseerd worden volgens het type inhoud erin aanwezig: bibliografisch, full tekst, afbeeldingen, namen,...
Data breach	Zie "inbreuk in verband met persoonsgegevens".
Datamining	Omvat alle technologieën die erop gericht zijn informatie uit een databank te analyseren om relevante informatie te vinden alsook om eventuele belangrijke correlaties op te sporen die bruikbaar zijn tussen de gegevens.
Datawarehouse	Of gegevenswarenhuis. Databank gebruikt voor het verzamelen, ordenen, registreren en opslaan van informatie afkomstig van operationele data om zo de besluitvorming binnen de onderneming mee te ondersteunen.
DDoS	Distributed Denial of Service betekent dat de aanval vanaf meerdere computers wordt uitgevoerd. Een DDoS is een aanval gericht tegen een server bedoeld om de werking ervan plat te leggen en toegang voor legitieme gebruikers onmogelijk te maken. Een groot aantal geconnecteerde objecten ("botnet") neemt aan deze aanval deel. Door de toestroom van een enorme hoeveelheid informatie die de aangevallen server plots moet beheren, kan die de talloze verzoeken niet meer behandelen en is die dan ook niet meer bereikbaar.
Derde	Art.4, §10 GDPR "Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken."

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Domain Name System (DNS)	Art. 4, § 14 NIS-richtlijn *"Hiërarchisch opgebouwd adresseringssysteem in een netwerk dat een zoekvraag naar een domeinnaam beantwoordt"* Systeem, van essentieel belang voor de werking van internet, dat helpt om het correcte IP-adres bij een domeinnaam te vinden. Bijvoorbeeld, het DNS stemt het domein van de website van de FOD Economie af op ons IP-adres. Dankzij DNS hoeft u ons IP-adres niet te weten om ons te vinden.
Doorgifte van (persoons)gegevens	Art. 44 tot 50 GDPR + overweging 101 tot 116 Persoonsgegevens die worden verwerkt of die zijn bestemd om na doorgifte aan een derde land of een internationale organisatie te worden verwerkt, mogen slechts worden doorgegeven indien aan bepaalde voorwaarden is voldaan (zie artikelen 44 tot 50 van de GDPR).
DPIA	Art. 35 en 83, §4, a GDPR + overweging 75, 84, 89 tot 93 Data Protection Impact Analysis of Impactanalyse m.b.t. de bescherming van persoonsgegevens. "Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, voert de verwerkingsverantwoordelijke voor de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden."
Dropper	Parasietsoftware (type Trojaans paard) die andere schadelijke software levert, uitpakt en installeert.

Drown Attack	Drown attacks stellen cyberaanvallers in staat om informatie vast te leggen tussen een gebruiker en een https-website. De https zorgt er a priori voor dat het een beveiligde site is. Bij verdrinkingsaanvallen worden echter serverkwetsbaarheden gebruikt die verouderde SSLv2- (TLS-voorgangers) technologieën ondersteunen. Om dit soort aanvallen te bestrijden, is het nodig om een recente cryptografiesleutel te gebruiken. Geen TLS-server mag een SSL-versie gebruiken. Zie voor meer informatie: https://drownattack.com/ Zie ook: https://www.enisa.europa.eu/publications/info-notes/the-drown-attack
DRP (Disaster Recovery Plan)	Dankzij een Disaster Recovery Plan kan een activiteit snel worden hervat na een catastrofe (overstroming, brand, onverwachte stroomuitval, ...), in elk geval voor de kritieke opdrachten van de onderneming. Het DRP identificeert welke activiteiten eerst moeten worden hervat, bepaalt ieders rol en geeft de te volgen procedures aan. Zie ook "BCP".

E

EBIOS	De EBIOS-methode ("Expression des Besoins et Identification des Objectifs de Sécurité ", of uiting van de benodigdheden en identificatie van de beveiligingsdoelen) is een Frans instrument (ANSSI). EBIOS zorgt voor een tamelijk uitgebreid beheer van de beveiligingsrisico's bij informatiesystemen en voldoet aan internationale normen zoals ISO/IEC 27001, ISO/IEC 27005 en ISO/IEC 31000.
ECSO (European Cyber Security Organisation)	Non-profitvereniging die de belangen van de particuliere sector, de academische sector en de publieke sector vertegenwoordigt bij de Europese Commissie inzake cyberbeveiliging. ECSO ondersteunt Europese initiatieven en projecten om cybersecurity in Europa te ontwikkelen, aan te moedigen en te bevorderen. Ze is onderverdeeld in verschillende werkgroepen en biedt verschillende sectoren en bedrijven de mogelijkheid om hun mening te geven en informatie uit te wisselen.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

e-government (e-Gov)	Bestaat erin om dienstverlening van overheidsdiensten richting burgers, ondernemingen, andere administraties enzovoort geheel of gedeeltelijk elektronisch te laten verlopen. Met de tax-on-web applicatie in België, bijvoorbeeld, kunnen burgers zelf hun belastingaangifte via internet invullen.
e-health	Belgisch platform voor informatie- en communicatietechnologieën binnen de volksgezondheid.
Encryptie	Zie versleuteling.
ePrivacy Regulation	Toekomstige Europese verordening ter vervanging van Richtlijn 2002/58, bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie.
ERP (Enterprise Resource Planning)	Soms "geïntegreerde bedrijfssoftware" genoemd. ERP is een geïntegreerd systeem voor het optimaliseren van de beheerprocessen door alle applicaties te bundelen, van boekhouding en beheer van personele middelen tot projectmanagement en logistiek. Middelen worden gedeeld en de verschillende diensten binnen de onderneming hebben realtime toegang tot geactualiseerde databanken. De meest bekende zijn SAP, Oracle, Sage, Microsoft Business Solutions, Generix, ...
Escalarematrix	Een escalarematrix is een plan of procedure die het hoofd moet bieden aan potentiële problemen in diverse contexten. De escalarematrix identificeert wie gecontacteerd moet worden naargelang de ernst (impact) van het geïdentificeerde incident of probleem alsook de vereiste operationele en/of beslissingscapaciteiten (strategisch) om het probleem op te lossen en/of de communicatie naar buiten toe te regelen.
Europees Comité voor gegevensbescherming	Voorheen "G 29" (WP29). Het Europees Comité bestaat uit het hoofd van een toezichthoudende autoriteit van elke lidstaat en de Europese Toezichthouder voor Gegevensbescherming (EDPS), of hun respectievelijke vertegenwoordigers. Dit comité geeft richtsnoeren, aanbevelingen en goede praktijken voor de implementatie van de GDPR.

F

Firewall	Tool voor het reguleren van het verkeer tussen het interne netwerk en internet. Hardware/software die de doorstroming van het netwerkverkeer regelt via een reeks vooraf vastgestelde regels en met bepaling van soort geautoriseerde toegang. Zie ook "WAF".
Forensic(s)	Toepassing van wetenschappelijke technieken en methoden op strafbare feiten. In cyberaangelegenheden gaat het erom dat bewijsmateriaal voor cyberaanvallen kan worden bewaard en geanalyseerd. Deze methoden worden zowel door overheden (FCCU, CERT,...) als door bedrijven toegepast om cyberaanvallers te identificeren, maar ook om cyberaanvallen effectiever te bestrijden door er lessen uit te trekken.

G

G29 (artikel 29-werkgroep) (WP29)	Oude benaming voor het Europees Comité voor gegevensbescherming (zie art. 29 van Richtlijn 95/46). Zie ook Europees Comité voor gegevensbescherming.
GDPR	General Data Protection Regulation Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).
Gegevensbeschermings-autoriteit (GBA)	Voorheen Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL). De Belgische toezichthouder voor de verwerking van persoonsgegevens, die toeziet op de naleving van de regels van de Europese Verordening 2016/679 (GDPR).

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

	Zie ook: Wet van 3 december 2017 tot oprichting van de gegevensbeschermingsautoriteit. Officiële website: https://www.gegevensbeschermingsautoriteit.be/
Geolokalisatie	Geolokalisatie omvat een reeks technische processen waarmee het mogelijk is om personen, in de meeste gevallen in realtime, geografisch te lokaliseren. Geolokalisatietechnieken werden eerst gebruikt om de geografische locatie van internetgebruikers op pc (IP-geolokalisatie) te bepalen om dan later veelvuldig te worden ingezet bij mobiele telefoons en applicaties.
Gevoelige gegevens (bijzondere categorie)	Art. 4, 6, 9, 36, 83, §5,a en 89 GDPR + overweging 51 tot 56 De verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religie of overtuiging, of het lidmaatschap van een vakvereniging blijkt, en de verwerking van genetische gegevens, biometrische gegevens voor identificatie van een natuurlijke persoon op unieke wijze, gegevens over gezondheid of seksleven of seksuele geaardheid van een natuurlijk persoon, zijn verboden (zie art. 9 GDPR).

H – I

Hardware	Met hardware wordt de computerapparatuur in het algemeen aangeduid, in tegenstelling tot software, wat verwijst naar programma's en programmatuur.
HTTPS	Hypertext Transfer Protocol Secure. Dit symbool linksboven in de zoekbalk betekent dat de verbinding in principe veilig is.
(IaaS) Infrastructure as a Service	Vorm van cloudcomputing die de onderneming toestaat om van de cloudprovider materiële abstracte hulpbronnen (doorgaans virtuele machines) te verkrijgen waarmee hij op het gewenste moment over al de nodige rekenkracht, opslagcapaciteit of communicatiesnelheid kan beschikken.

(IAM) Identity and Access Management	Identiteits- en toegangsbeheer. IAM is een beveiligingsoplossing om de lijst van gebruikers centraal te beheren en hun toegangsrechten te identificeren.
IDS (Intrusion Detection System)	Een IDS is een inbraakdetectiesysteem dat verdachte activiteiten in het netwerk bewaakt. IDS waarschuwt de beheerders, maar blokkeert geen aanvallen (zie IPS). Sommige IDS'en kunnen worden geconfigureerd om schendingen van uw veiligheidsbeleid op te sporen.
Inbreuk in verband met persoonsgegevens	Art. 4, §12; 33 en 34 GDPR + overweging 73 en 85 een inbreuk op de beveiliging of "data breach" die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.
Incident	Art. 4 NIS-richtlijn *"Elke gebeurtenis met een daadwerkelijk schadelijk effect op de beveiliging van netwerk- en informatiesystemen."* Een Incident Management Plan is een plan voor incidentbeheer.
Indicators of Compromise (IoC)	Middel dat (bijna) automatisch op zoek gaat naar bedreigingen binnen het netwerk. IoC's alleen zijn niet voldoende om incidenten of problemen op te sporen maar ze vormen wel een eerste detectiemethode.
Insider Threat	Een medewerker of een groep medewerkers binnen een organisatie die een IT-bedreiging vormen door de beveiligingsregels, al dan niet met opzet, te overtreden.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

IoT (Internet of Things)	Refereert aan geconnecteerde fysieke objecten met hun eigen digitale identiteit en in staat om onderling te communiceren. Dit netwerk creëert als het ware een brug tussen de fysieke en virtuele werkelijkheid. Een aangesloten horloge, een aangesloten bril, een aangesloten camera en slimme meters zijn allemaal voorbeelden van IoT.
IP of Internet Protocol (IPv4, IPv6)	Internetcommunicatie is gebaseerd op een protocol dat computers in staat stelt met elkaar te communiceren. Dit protocol wordt IP voor Internet Protocol genoemd. Elke aangesloten machine onderscheidt zich van de andere door een numeriek adres. Communicatie tussen machines gebeurt door informatiepakketten te versturen die elk een bron- en een bestemmingsadres bevatten. Er bestaan verschillende versies (v) van het IP-protocol. Momenteel wordt IPv6 ingezet (8 groepen van 4 hexadecimale cijfers), ook al zijn er nog veel machines via IPv4 verbonden. IPsec is een protocol voor het versleutelen en ondertekenen van IP-pakketten.
IP-adres	Identificatienummer permanent of tijdelijk toegekend aan elk apparaat dat verbonden is met een computernetwerk en gebruikmaakt van het Internet Protocol (IP).
IPS (Intrusion Prevention System)	Een IPS houdt het netwerkverkeer in de gaten en laat toe om, in geval van aanval, de gegevens te analyseren m.b.t. de aanval en de nodige corrigerende maatregelen te nemen (bv. door de firewall van de onderneming aan te passen).
ISP (Internet Service Provider)	Ook internetaanbieder genoemd. Een ISP biedt internetverbinding alsook eventuele bijkomende diensten (e-mailadres, ...)

ITIL	Information Technology Infrastructure Library (ITIL). Referentiekader met een reeks van best practices voor het inrichten van een efficiënt beheer van het informatiesysteem.
IXP (internetknooppunt)	Art. 4, § 13 NIS-richtlijn "een netwerkinfrastructuur die de onderlinge verbinding van meer dan twee onafhankelijke autonome systemen mogelijk maakt, voornamelijk met als doel de uitwisseling van internetverkeer te vergemakkelijken; een internetknooppunt zorgt voor onderlinge verbinding enkel voor autonome systemen; een internetknooppunt vereist niet dat het internetverkeer tussen twee deelnemende autonome systemen via een derde autonoom systeem verloopt noch dat het internetknooppunt dergelijk verkeer wijzigt of anderszins daartussen komt."

J – K – L

Key logger	Software/hardware die discreet de bewegingen (tablets) of toetsaanslagen registreert om informatie te stelen (bestanden, wachtwoorden, geheime codes, ...).
Kritieke infrastructuur	Art. 3 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren "installatie, systeem of een deel daarvan, van federaal belang, dat van essentieel belang is voor het behoud van vitale maatschappelijke functies, de gezondheid, de veiligheid, de beveiliging, de economische welvaart of het maatschappelijk welzijn, en waarvan de verstoring van de werking of de vernietiging een aanzienlijke weerslag zou hebben doordat die functies ontregeld zouden raken."
LDPA	LDPA (Lightweight Directory Access Protocol) is een toepassingsprotocol om elementen in de database van informatiediensten op te vragen en te wijzigen, zoals Active Directory (AD).

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

M – N – O

Malware

Schadelijke software. Software die het goed functioneren van een informatiesysteem in gevaar brengt door niet-geautoriseerde taken en processen uit te voeren.
Zie ook "ransomware" en "Trojaans paard".

MEHARI

MEHARI (MEthod for Harmonized Analysis of RIsk) is een gratis methode (open source) om risicoanalyses en risicobeheersanalyses uit te voeren die conform de ISO/IEC 27001:2013 en ISO/IEC 27005:2011 normen zijn.

Metadata

Informatie die de karakteristieken van bepaalde gegevens beschrijft. Bij een e-mail zijn relevante metadata bijvoorbeeld de naam van de afzender, de naam van de bestemmeling, het tijdstip waarop de e-mail is verzonden, ... dit in tegenstelling tot de gegevens in het bericht zelf, in dit voorbeeld de inhoud van de e-mail.

Mitigeren (mitigatie)

Mitigeren van risico's: middelen en maatregelen die in werking worden gesteld om de kans op een bedreiging en/of gevolgen ervan te beperken.

Modelcontract-bepalingen

Modelcontractbepalingen aangenomen door de Europese Commissie of door de nationale toezichthouder. Ze zijn bedoeld om de taken van de verwerkingsverantwoordelijke op het gebied van de uitvoering van contracten te vergemakkelijken m.n. voor het verzenden van persoonsgegevens buiten de Europese Unie of in de relatie tussen verwerkingsverantwoordelijke en verwerker (zie art. 46 en 28 GDPR).

MONARC

Monarc is een gratis en geoptimaliseerde Luxemburgse methode voor het voeren van een risicoanalyse. Dankzij deze methode kan een volledig rapport inzake risico's worden uitgewerkt en kunnen mogelijke oplossingen worden geïdentificeerd.

NIS	Security of Network and Information Systems. Engelstalige afkorting die verwijst naar de Richtlijn 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.
NIST	National Institute of Standards and Technology (U.S Department of Commerce).
Ontvanger	Art. 4, §9 GDPR + overweging 31 "Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het lidstatelijke recht gelden echter niet als ontvangers; de verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn"
Open Data	Gegevens die voor iedereen direct toegankelijk zijn. De data is vrij van auteursrechten en omvat geen voorafgaande controle. Zo worden werkgelegenheidsstatistieken bijvoorbeeld beschouwd als open data (data.gov.be).
Opensourcesoftware	Software verkocht met een broncode en een licentie waarbij het wettelijk is toegestaan om de software te kopiëren, te verkopen of te verspreiden, zonder bijkomende kosten voor de oorspronkelijke aankoper. Deze licentie verhindert in principe dat particuliere belanghebbenden opensourcesoftware gaan gebruiken en wijzigen en er een eigen product van zouden maken.
Operating System (OS)	Het besturingssysteem dat ervoor zorgt dat alle applicaties naar behoren functioneren en dat gebruikers makkelijk met de programma's kunnen werken.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Opt-in/Opt-out

De termen opt-in/opt-out verwijzen naar verschillende methoden waarbij de betrokkene de verwerking van zijn persoonsgegevens kan weigeren. Opt-in betekent dat de betrokkene vooraf zijn toestemming moet kenbaar maken. Opt-out houdt dan weer in dat de verwerking standaard gebeurt en dat de betrokkene duidelijk moet aangeven om hieraan een einde te maken door actief te handelen. Een lijst zoals "bel-me-niet-meer" is van het type "opt-out". Personen die ingeschreven staan in het bel-me-niet-meer-register worden niet meer telefonisch benaderd voor commerciële doeleinden.

P

PaaS (Platform as a Service)

De onderneming koopt bij de cloudprovider de toegang tot een ontwikkelingsplatform. Dit is een specifieke omgeving waarbinnen de onderneming applicaties kan schrijven en testen die op dit platform of op een soortgelijke installatie draaien. Het platform (middleware) bepaalt de standaarden waarmee men op een ruime en interactieve wijze talrijke klanten kan bereiken en hun keuze qua software kan uitbreiden.

Patch

Een patch omvat het geheel van wijzigingen, aan te brengen in een softwareprogramma en dient m.n. om de betrokken software up-to-date te houden, bepaalde zwaktes te corrigeren of om bepaalde criteria te verbeteren (vermogen, gebruiksvriendelijkheid, ...).

Persoonsgegevens

Art. 4, §1 GDPR + overweging 26 tot 29 en 38
"Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online-identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon."

Phishing	Vorm van social engineering (e-mails) bedoeld om sleutelinformatie te vergaren (wachtwoorden, bankrekeningnummers, bedrijfsrekeningen, ...).
PNR	Passenger Name Record Wet van 25 december 2016 betreffende de verwerking van passagiersgegevens.
Prince2	Procesgeoriënteerde methode voor projectmanagement.
Privacy Policy	Een "privacy policy" of "beleid m.b.t. de vertrouwelijkheid van (persoons)gegevens" is een juridisch document dat preciseert op welke manier de verwerkingsverantwoordelijke om moet gaan met het gebruik, verspreiding en beheer van de persoonsgegevens van een betrokkene (klant). De privacy policy laat m.n. toe om te beantwoorden aan de wettelijke transparantieverplichting die rust op de verwerkingsverantwoordelijke.
Privileged Identity Management (PIM)	Systeem voor het beheer van geprivilegieerde accounts (IT-beheerders, ...).
Profilering	Art. 4, §4 GDPR + overweging 30 en 91 "Elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen."
Proportionaliteitsbeginsel	Het proportionaliteitsbeginsel houdt in dat persoonsgegevens slechts worden verwerkt voor zover ze, "gelet op de doeleinden waarvoor ze worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn". Dit betekent dat enkel relevante en noodzakelijke gegevens mogen worden verzameld.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Proxy

Een "proxy" is een specifiek systeem of software voor op de computer die als tussenschakel werkt tussen een eindterminal (bv. een computer) en een andere server op welke een gebruiker of klant een dienst kan aanvragen. Een proxy kan m.n. toestaan om op een "anonieme" manier te surfen op het internet.

Pseudonimisering

Art.4, §5 GDPR + overweging 26, 28, 29
"Het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld".

PUP

Potentially Unwanted Programs
Potentieel ongewenste software die vaak meelift met "gratis" applicaties. Dit kan pop-ups (adware) laten verschijnen, wijzigingen aan de werkbalk aanbrengen, de homepage veranderen en/of achtergrondtaken uitvoeren die de prestaties van computers vertragen.

Q – R

Ransomware

Ransomware is schadelijke software die gegevens versleutelt op het geïnfecteerde toestel en dat belooft om de gegevens opnieuw toegankelijk te maken mits er losgeld wordt betaald (in bitcoins).
Zie: https://www.nomoreransom.org/ en https://ransomfree.cybereason.com/

Rechtmatige verwerking

Art. 5, 6, 83, §5, a GDPR + overweging 40 tot 50
De verwerking van persoonsgegevens moet voldoen aan de voorwaarden van artikel 5 van de GDPR. Tot die voorwaarden behoort de rechtmatige verwerking (zie artikel 6 van de GDPR).

Rechtmatigheid van de verwerking	Zie rechtmatige verwerking.
Recht op informatie	Art. 12 tot 14 GDPR + overweging 58 tot 62 "Overeenkomstig de beginselen van behoorlijke en transparante verwerking moet de betrokkene op de hoogte worden gesteld van het feit dat er verwerking plaatsvindt en van de doeleinden daarvan. De verwerkingsverantwoordelijke dient de betrokkene de nadere informatie te verstrekken die noodzakelijk is om tegenover de betrokkene een behoorlijke en transparante verwerking te waarborgen, met inachtneming van de specifieke omstandigheden en de context waarin de persoonsgegevens worden verwerkt. De betrokkene heeft (niet absoluut) recht op toegang tot informatie die hij in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal moet ontvangen".
Recht op rectificatie	Art. 5, 12, 19 en Art. 16, art. 83, §5, b GDPR, + overweging 65 De betrokkene heeft het recht om van de verwerkingsverantwoordelijke onverwijld rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen. Met inachtneming van de doeleinden van de verwerking heeft de betrokkene het recht vervollediging van onvolledige persoonsgegevens te verkrijgen, onder meer door een aanvullende verklaring te verstrekken.
Recht op vergetelheid (Recht op gegevenswissing)	Art. 6, 8, 9, 12,15, 17, 19, 21, 83, §5, b, 89 GDPR + overweging 65 en 66 De betrokkene heeft onder bepaalde voorwaarden het recht om van de verwerkingsverantwoordelijke zonder onredelijke vertraging wissing van zijn persoonsgegevens te verkrijgen en de verwerkingsverantwoordelijke is verplicht om persoonsgegevens zonder onredelijke vertraging te wissen (zie artikel 17 GDPR).

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Recht van bezwaar	Art. 5, art. 6, §1, e) en f), art. 12; art. 21, art. 83, §5, b GDPR + overweging 69 en 70 De betrokkene heeft te allen tijde het recht om vanwege met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens op grond van de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is, met inbegrip van profilering op basis van die bepalingen. De verwerkingsverantwoordelijke staakt de verwerking van de persoonsgegevens tenzij hij dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering.
Recovery (of herstel)	Dit kan betrekking hebben op een opslagpunt dat toelaat om in geval van systeemfalen terug te keren naar een toestand voorafgaand aan het falen (herstelpunt). Het kan ook betrekking hebben op een plan zoals het Disaster Recovery Plan dat voorziet hoe men kritieke taken moet verzekeren in geval van een ramp (catastrofe).
RFID (Radio Frequency IDentification)	Methode gebruikt om gegevens op te slaan en te recupe-reren vanop afstand door gebruik te maken van metalen labels, die gekleefd kunnen worden op of geincorpo-reerd kunnen worden in de producten.
Richtlijn 2002/58	Zal binnenkort worden vervangen door de ePrivacy Regulation

	Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie).
Richtlijn 95/46	Vervangen door de GDPR (25 mei 2018) Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.
Risico	Elke redelijkerwijs vast te stellen omstandigheid of gebeurtenis met een mogelijk schadelijk effect op de beveiliging van netwerk- en informatiesystemen.

S

SaaS (Software as a Service)	Vorm van cloudclomputing waarbij de onderneming een complete en operationele applicatie koopt tot welke de gebruiker toegang krijgt via zijn webbrowser of via een andere client-software. Met deze wijze van softwaregebruik, verdwijnt of vermindert de noodzaak om op elk toestel van de klant software te installeren.
SIEM	Security Information and Event management. Met SIEM-tools kan informatie op het netwerk worden samengevoegd, geordend en vergeleken (correleren). Dit om verdachte activiteiten op te sporen door monitoren van applicaties, gebruikersgedrag en toegang tot gegevens. Maar baseer uw verdediging niet alleen daarop en vergeet niet dat de kwaliteit van de detectie- en correlatieregels, de dekking van de incidenttypes en de responsprocessen bij detectie ook op een doeltreffende manier moeten worden geïmplementeerd.

SLA (Service Level Agreement)	Een SLA is een contract of een deel van het contract voor het vastleggen van de verwachte serviceniveaus waarbij er aan elk serviceniveau mogelijke sancties worden gekoppeld. Een SLA bepaalt de (voornaamste) behoeften van de begunstigde, schept duidelijkheid voor beide partijen, legt doelstellingen zonder onrealistische verwachtingen vast en kan een inspanningsverplichting omzetten in een resultaatsverplichting. Een SLA kan door de verkoopafdeling van een onderneming ook worden aangewend als marketingtool ten aanzien van begunstigden.
SLM	De Service Level Manager (SLM) is een beheerder die zich ervan verzekert dat de verwachte niveaus van interne en externe dienstverlening geïdentificeerd worden en erover waakt dat deze niveaus worden gerespecteerd. De SLM werkt samen met de interne en externe diensten, om erop toe te zien dat alle beheersprocessen van de informaticadiensten die deze niveaus verzekeren, gerespecteerd worden.
Smart grids	"Slim netwerk" dat netbeheerders in staat stelt om de energiestromen te controleren en hun prijzen aan te passen op basis van vraag en aanbod. Gekoppeld aan een slimme meter, kan een smart grid ook bij de consument zijn nut bewijzen door hem in realtime informatie betreffende verbruik te bezorgen en hem in staat te stellen zijn kosten bij te sturen.
Software	Programma's en procedures noodzakelijk voor de werking van computersystemen (in tegenstelling tot hardware). Zie ook "applicatie". Schadelijke software wordt "malware" genoemd (zie ook "malware").
Softwarepakket	Zie software.

Sybil Attack	Het gaat om het beschadigen van de onlinereputatie van een leverancier van goederen of diensten. In het geval van een "sybil"-aanval maakt de aanvaller meerdere identiteiten of profielen aan en gebruikt hij meerdere accounts om de reputatiescores van een bedrijf of onlinedienst te manipuleren. De reputatie van een site kan op die manier kunstmatig worden opgeblazen of juist worden beschadigd zonder dat er een concreet verband met de werkelijkheid bestaat.

T

(TLP) Traffic Light Protocol	Classificatie- en indelingssysteem voor gegevens op basis van kleurcode (doorgaans 4 kleuren: rood, oranje, groen, wit) om ervoor te zorgen dat de informatie niet in de handen van verkeerde personen terechtkomt.
Toegangsrecht	Art. 15, 30, 83, §5, b GDPR + overweging 63 en 64 De betrokkene heeft het recht om van de verwerkingsverantwoordelijke uitsluitsel te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen van die persoonsgegevens en van bepaalde informatie (zie artikel 15 GDPR).
Toestemming van de betrokkene	Art. 4, §11 GDPR en art. 6, 7 en 83, §5, a + overweging 32, 33, 38, 42 en 43 "elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt." Opgelet: de betrokkene kan, in vele gevallen, zijn toestemming intrekken.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Transparantie

Art. 5, art. 12 tot 14 en 15 tot 22, art. 34 GDPR + overweging 58 en 59

De verwerkingsverantwoordelijke neemt passende maatregelen opdat de betrokkene de in de artikelen 13 en 14 bedoelde informatie en de in de artikelen 15 tot en met 22 en artikel 34 bedoelde communicatie in verband met de verwerking in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal ontvangt, in het bijzonder wanneer de informatie specifiek voor een kind bestemd is. De informatie wordt schriftelijk of met andere middelen, met inbegrip van, indien dit passend is, elektronische middelen, verstrekt. Indien de betrokkene daarom verzoekt, kan de informatie mondeling worden meegedeeld, op voorwaarde dat de identiteit van de betrokkene met andere middelen bewezen is.

Trojaans paard

Computerprogramma (of malware) dat zich voordoet als legitieme software maar verborgen functies met kwade bedoelingen bevat.

U – V – W – X – Y – Z

URL

Uniform Resource Locator. Middel waarmee informatie op het web kan worden gevonden (www).

Versleuteling

Art.2, §40 van de WEC

"alle diensten die de beginselen, middelen en methodes voor de omzetting van gegevens aanwenden met de bedoeling de semantische inhoud ervan te verbergen, de authenticiteit ervan vast te stellen, te verhinderen dat zij onopgemerkt worden gewijzigd, te verhinderen dat zij worden verworpen en te verhinderen dat zij zonder toestemming worden gebruikt."

Afgeleid van het Griekse woord κρυπτός (cruptos) dat "verstopt, verborgen" betekent en van γράφειν (graphein) dat "schrijven" betekent. Versleuteling staat voor het coderen van gegevens (teksten, berichten, ...) aan de hand van een "sleutel" om de gegevens voor iedereen, behalve de persoon aan wie het bericht gericht is, onherkenbaar te maken.

	Het proces om de originele informatie via de versleutelde tekst terug te vinden, wordt decryptie genoemd.
Verwerker	Art.4, §8 en art. 28 GDPR + overweging 81 "Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt."
Verwerking (van persoonsgegevens)	Art. 4, §2 GDPR Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
Verwerkingsdoel	Beoogde doelstellingen van één/reeks bewerkingen van gegevens. Verwerkingsdoelen van persoonsgegevens moeten voldoen aan de criteria van artikel 5, §1, b GDPR.
Verwerkingsverantwoordelijke	Art. 4, §7 GDPR + art. 24 tot 43 een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen
Videobewaking/ videobescherming	Zie bewakingscamera's.

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

VPN	Virtual Private Network. Met VPN kunt u een beveiligde verbinding tot stand brengen door de communicatie tussen uw computer en de server van uw bedrijf te versleutelen. Bijvoorbeeld: u beschikt over een onveilige wifiverbinding (openbare wifi van een hotel, station,...) en u wilt professionele gegevens van uw bedrijf verzenden en/of ontvangen. Als u via een VPN verbinding maakt, ziet de wifirouter waarop u bent aangesloten alleen versleutelde gegevens passeren en zullen uw bedrijfsgegevens beschermd blijven.
WAF	Web Application Firewall. Naast het fungeren als standaardfirewall, kan een WAF eveneens content filteren, spam bestrijden, hackpogingen opsporen en bepaalde virussen detecteren. Zie ook "Firewall".
Web (www)	World Wide Web of "Web" wat letterlijk "(spinnen) web" betekent en dient ter omschrijving van het "internet".
WEC	Wet van 13 juni 2005 betreffende de elektronische communicatie.
Wifi	Draadloze internetverbinding.
WPL	Oude Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (omzetting van de oude Richtlijn 95/46). Zie "GDPR"
Zombie	Zie Botnet.