Handleiding gegevensbescherming en privacy

Versie 1.0 , november 2018

Stafdiensten
Huis van het GO!
Willebroekkaai 36
1000 Brussel

1. Inleiding

Op 27 april 2016 werd de Algemene Verordening Gegevensbescherming[1] aanvaard door het Europees parlement en de raad van de Europese Unie (afgekort AVG of GDPR[2]). Deze verordening heeft rechtstreekse werking. Dat wil zeggen dat ze rechtsreeks van kracht is in de lidstaten zonder dat deze daarvoor eigen wetgevende initiatieven moeten nemen.

De AVG bevat een stelsel van verplichtingen die worden opgelegd aan elke organisatie die de persoonsgegevens van natuurlijke personen verwerkt. De doelstelling van de verordening is enerzijds het harmoniseren van de bescherming van de grondrechten en de fundamentele vrijheden van natuurlijke personen in verband met verwerkingsactiviteiten, en anderzijds het vrije verkeer van persoonsgegevens binnen de Unie te waarborgen.

Aangezien de bescherming van persoonsgegevens uitdrukkelijk een onderdeel uitmaakt van de grondrechten en fundamentele vrijheden van natuurlijke personen kan het belang van het respecteren van deze regelgeving niet worden onderschat.

Deze handleiding beoogt een houvast te zijn voor alle personeelsleden binnen het GO! bij het naleven van het regelgevend kader die de door de AVG werd ingevoerd.

In een eerste deel wordt verduidelijkt hoe de verschillende actoren binnen het GO! elk vanuit hun bevoegdheid dienen om te gaan met de verplichtingen die de AVG aan het GO! oplegt, en op welke wijze de communicatie en samenwerking tussen de verschillende bestuursniveaus moet vormgegeven worden.

In het tweede deel worden de procedures beschreven die moeten worden gevolgd bij enerzijds het melden en afhandelen van een beveiligingsincident of gegevenslek en anderzijds het uitoefenen door de betrokkende van de hem door de AVG toegekende rechten.

In het derde deel worden inhoudelijke en concrete richtlijnen meegegeven. Van alle GO! personeelsleden wordt gevraagd deze richtlijnen maximaal na te leven. De bedoeling hiervan is dat we met zijn allen bijdragen aan de veilige verwerking van de persoonsgegevens die ons toevertrouwd worden.

[1] Voluit de E.U. Verordening 2016/679 van het Europees Parlement en de Rad 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 .

[2] G.D.P.R. is de afkorting van de Engelse benaming van de verordening. Dit staat voor General Data Protection Regulation.

2. Taakverdeling

De AVG legt aan ieder die persoonsgegevens verwerkt regels op waaraan deze verwerkingen moeten voldoen. Die regels brengen binnen de context van onderwijsverlening en het GO! in het bijzonder een aantal bijkomende taken met zich mee.

Deze taken worden in dit hoofdstuk beschreven, uitgesplitst volgens de drie bestuursniveaus van het GO!.

2.1. Rollen op het lokale niveau

2.1.1. Directeur

2.1.1.1. De directeur staat in voor het opstellen van het beleid aangaande informatieveiligheid en de bescherming van persoonsgegevens binnen zijn instelling

- Voegt in het schoolreglement onderdeel bescherming van persoonsgegevens toe (sjabloon aan te leveren door centrale diensten)
- Invullen en bijhouden register van verwerkingsactiviteiten / incidentenregister
  - Dit gebeurt binnen sjabloon aangeleverd door Centrale diensten (IVOS-tool)
  - Ingevuld register is ter inzage van algemeen directeur en aanspreekpunten informatieveiligheid scholengroep en van data protection officer (functionaris gegevensbescherming) centrale diensten (via IVOS-tool)
- Inventarisatie van verwerkers (extern) en nagaan of met hen een verwerkingsovereenkomst werd afgesloten. Indien geen verwerkingsovereenkomst: opmaak conform sjabloon aangeleverd door Centrale diensten (in samenspraak met aanspreekpunt)
- Bewustmaking en monitoring personeelsleden aangaande omgaan met persoonsgegevens
  - Bewustmaking over policies aangaande informatieveiligheid /omgaan met persoonsgegevens (aangeleverd door centrale diensten)
  - Naleving van deze policies bijhouden en rapportering aan aanspreekpunt scholengroep

De directeur kan de uitvoering van deze taken delegeren. Hij draagt evenwel de formele verantwoordelijkheid.

2.1.1.2. De directeur fungeert als formeel contactpunt voor privacy-gerelateerde aangelegenheden en wordt zo aangeduid in schoolreglement / privacyverklaring

- Meldpunt voor gegevenslekken binnen zijn instelling
  - Na kennisname van gegevenslek zo snel mogelijk alle feitelijke info verzamelen d.m.v. vragenlijst aangeleverd door data protection officer / functionaris gegevensbescherming centrale diensten (IVOS-tool)
  - Deze info onmiddellijk doorsturen naar aanspreekpunt informatieveiligheid scholengroep
- Instaan voor registratie voor incidenten / gegevenslekken binnen zijn instelling, hiervoor kan hij een beroep doen op ondersteuning aanspreekpunt informatieveiligheid van de scholengroep
- Staat in afhandeling van privacy-gerelateerde vragen en uitoefening rechten van betrokken (recht op inzage, verwijdering, …), hiervoor kan hij een beroep doen op ondersteuning aanspreekpunt

De directeur kan de uitvoering van deze taken delegeren. Hij draagt evenwel de formele verantwoordelijkheid.

2.1.1.3. De directeur staat in voor het handhaven van het beleid aangaande informatieveiligheid en de bescherming van persoonsgegevens binnen zijn instelling

- Input van aanspreekpunt aangaande de opvolging van het beleid ter harte nemen
- Klachtenbehandeling volgens de gangbare procedures (klacht / orde en tucht)
- Hierover jaarlijks verslag uitbrengen aan de raad van bestuur (bv. in het jaarverslag)

De directeur kan de uitvoering van deze taken niet delegeren.

2.1.1.4. De directeur heeft een beslissende rol bij risicoanalyse

- Dit gebeurt met ondersteuning van aanspreekpunt informatieveiligheid scholengroep

De directeur kan de uitvoering van deze taken niet delegeren.

2.1.2. Personeelsleden van de lokale instellingen

2.1.2.1. Naleven richtlijnen aangaande informatieveiligheid

2.1.2.2. Meldplicht informatieveiligheidsincidenten en gegevenslekken

2.2. Rollen op het mesoniveau

2.2.1. Algemeen Directeur

2.2.1.1. De algemeen directeur staat in voor het opstellen van het beleid aangaande informatieveiligheid en bescherming van persoonsgegevens binnen de scholengroep

- Invullen en bijhouden register van verwerkingsactiviteiten / incidentenregister
  - Dit gebeurt binnen sjabloon aangeleverd door Centrale diensten
  - Ingevuld register is ter inzage van DPO centrale diensten
- Inventarisatie van verwerkers (extern) en nagaan of met hen een verwerkingsovereenkomst werd afgesloten. Indien geen verwerkingsovereenkomst: opmaak conform sjabloon aangeleverd door Centrale diensten
- Toezicht op verwerkingsactiviteiten lokale instellingen en het niveau van de scholengroep
  - Register gegevensverwerkingen, incidentenregister

De algemeen directeur delegeert de uitvoering van deze taken aan het aanspreekpunt informatieveiligheid. Deze delegatie moet bekrachtigd worden door de raad van Bestuur van de scholengroep. De algemeen directeur draagt evenwel de formele verantwoordelijkheid.

2.2.1.2. De algemeen directeur staat in voor het handhaven van het beleid aangaande informatieveiligheid en de bescherming van persoonsgegevens binnen de scholengroep

- Input van aanspreekpunt aangaande de opvolging van het beleid ter harte nemen
- Klachtenbehandeling volgens de gangbare procedures (klacht / orde en tucht). Bij ontvangen klacht door DPO, wordt contact opgenomen met de algemeen directeur om te kijken wat moet gebeuren aan maatregelen en acties. De algemeen directeur schat in waar verder geëscaleerd moet worden

- Hierover jaarlijks verslag uitbrengen aan de raad van bestuur (bv. in het jaarverslag)

De algemeen directeur kan deze taak niet delegeren.

2.2.1.3. De algemeen directeur heeft een beslissende rol bij risicoanalyse

- Dit gebeurt met ondersteuning aanspreekpunt

De algemeen directeur kan deze taak niet delegeren.

2.2.1.4. De algemeen directeur wijst het aanspreekpunt informatieveiligheid aan

- Aanstelling aanspreekpunt melden aan data protection officer centrale diensten
- Wijziging aanspreekpunt melden aan data protection officer centrale diensten

De algemeen directeur kan deze taak niet delegeren.

2.2.2. Aanspreekpunt informatieveiligheid

2.2.2.1. Het aanspreekpunt informatieveiligheid geeft bijstand bij opstellen van het beleid aangaande informatieveiligheid en de bescherming van persoonsgegevens aan directeurs lokale instellingen en algemeen directeur scholengroep

- Bij invullen en bijhouden register van verwerkingsactiviteiten / incidentenregister in sjabloon aan te leveren door DPO centrale diensten (IVOS-tool)
- Bij afsluiten van verwerkingsovereenkomsten
- Bewustmaking directeurs lokale instellingen en personeel scholengroep rond policies aangaande omgaan met persoonsgegevens / informatieveiligheid (aangeleverd door centrale diensten)

2.2.2.2. Het aanspreekpunt heeft een ondersteunende rol bij risicoanalyses

- Dit gebeurt in samenspraak met directeurs lokale instellingen, respectievelijk algemeen directeur

2.2.2.3. Het aanspreekpunt fungeert als formeel contactpunt voor privacy-gerelateerde aangelegenheden

- Meldpunt voor incidenten en gegevenslekken binnen de scholengroep en bij de lokale instellingen
  - Na kennisname van gegevenslek (door personeelslid scholengroep of directeur instelling) zo snel mogelijk alle feitelijke info verzamelen d.m.v. vragenlijst aan te leveren door DPO centrale diensten (EVOS-tool)
  - Deze info z.s.m. door te sturen naar DPO Centrale diensten, die dan zal instaan voor melding aan Vlaamse Toezichtcommissie
  - Als melding niet tijdig kan gebeuren (72 u na gegevenslek) zelf reeds melding doen naar Vlaamse Toezichtcommissie , met melding dat ontbrekende informatie zal aangevuld worden door DPO Centrale diensten
- Instaan voor registratie van incidenten / gegevenslekken in incidentenregister binnen de scholengroep (IVOS-tool) en in deze materie ondersteuning geven aan lokaal niveau
- Fungeren als contactpunt voor vragen rond bescherming persoonsgegevens / informatieveiligheid,
  - Krijgt hierbij ondersteuning van DPO centrale diensten
- Staat in voor de afhandeling van uitoefening rechten van betrokken (recht op inzage, verwijdering, …) binnen de scholengroep en geeft in deze materie ondersteuning aan lokaal niveau
  - Krijgt hierbij ondersteuning van DPO centrale diensten

2.2.2.4. Het aanspreekpunt fungeert als contactpunt binnen de scholengroep voor de DPO

- Staat in voor verspreiding en implementatie binnen de scholengroep van de modeldocumenten die door centrale diensten worden aangeleverd
- Evalueert de wijze waarop de beleidsmaatregelen door de lokale instellingen en de scholengroep in de praktijk worden omgezet
- Aanspreekpunt signaleert risico's / pijnpunten aan de algemeen directeur die dit ter harte neemt en eventueel verder bij de Raad van Bestuur brengt
- Coördinator van de Informatieveiligheidscel van de scholengroep
- Participeert in Lerend Netwerk Informatieveiligheid

2.2.3. Informatieveiligheidscel van de scholengroep

De informatieveiligheidscel is een multidisciplinaire werkgroep die het aanspreekpunt informatieveiligheid bijstaat bij de concrete uitwerking van zijn taken.

2.2.4. Raad van bestuur

2.2.4.1. Beslissen over de beleidsmaatregelen binnen de scholengroep

2.2.4.2. Monitoren naleving richtlijnen en het nemen van de gepaste maatregelen

Monitoren naleving door directeurs en personeelsleden lokale instellingen.

Monitoren naleving door algemeen directeur en personeelsleden scholengroep.

2.2.4.3. AVG rolverdeling binnen de scholengroep: delegatie bevoegdheden van Algemeen Directeur bekrachtigen

2.2.5. Personeelsleden van de scholengroep

2.2.5.1. Naleven richtlijnen aangaande informatieveiligheid

2.2.5.2. Meldplicht informatieveiligheidsincidenten en gegevenslekken

2.3. Rollen op het centraal niveau

2.3.1. Data protection officer / Functionaris gegevensbescherming (DPO)

2.3.1.1. De DPO staat in voor de voorbereiding van het beleid aangaande informatieveiligheid en de bescherming van persoonsgegevens voor het GO!

- Richtlijnen, kaders, procedures en sjablonen opstellen en aanbevelingen doen m.b.t. gegevensbescherming
- Bijstand bij register van verwerkingsactiviteiten / incidentenregister
  - Aanleveren sjabloon en ondersteuning bieden bij invullen via IVOS-tool
  - Toezicht op ingevulde registers via IVOS-tool
- Inventarisatie van verwerkers (extern) en nagaan of met hen een verwerkingsovereenkomst werd afgesloten en aanlevering sjabloon
- Bewustmaking en monitoring personeelsleden aangaande omgaan met persoonsgegevens

- Bewustmaking over policies aangaande informatieveiligheid (inclusief aanlevering en bundeling van deze policies)
- Naleving van deze policies bijhouden en rapportering aan algemeen directeur scholengroepen en afgevaardigd bestuurder GO!, afhankelijk van de case
- Aanspreekpunten informatieveiligheids- en privacybeleid opleiden en hen de nodige instrumenten / hulpmiddelen verstrekken
- Lerend netwerk voor aanspreekpunten opzetten en aansturen

2.3.1.2. Handhaven van het beleid aangaande informatieveiligheid en de bescherming van persoonsgegevens binnen het GO!

- Input aangaande de opvolging van het beleid ter harte nemen
- Ondersteuning geven aan aanspreekpunten aangaande individuele dossiers
- Toezicht op verwerkingsactiviteiten lokale instellingen en scholengroepen
  - Register gegevensverwerkingen, incidentenregister

2.3.1.3. Adviserende rol bij risicoanalyse

- Kennis nemen van de registers van verwerkingsactiviteiten en incidentenregisters van alle niveaus
- Mogelijke risico's signaleren aan mesoniveau en de passende maatregelen voorstellen om deze risico's te beperken
- Advies verstrekken in het kader van een gegevensbeschermingseffectbeoordeling (een doorgedreven pro-actieve risico-beoordeling die in toepassing van art. 35 AVG in sommige gevallen verplicht is, onder andere bij de introductie van nieuwe technologieën die een verhoogd privacyrisico met zich kunnen meebrengen)[3]

2.3.1.4. Fungeren als formeel contactpunt voor privacy-gerelateerde aangelegenheden

- Meldpunt voor incidenten en gegevenslekken
  - Na kennisname van gegevenslek zo snel mogelijk alle feitelijke info verzamelen d.m.v. vragenlijst
  - Deze info z.s.m. melden aan de Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens (VTC)
- Ondersteuning bieden aan het mesoniveau bij de registratie van incidenten / gegevenslekken in het incidentenregister
- Ondersteuning bieden aan aanspreekpunten bij vragen rond bescherming persoonsgegevens / informatieveiligheid en bij de afhandeling van uitoefening rechten van betrokken
- Instaan voor de afhandeling van uitoefening rechten van betrokken die rechtsreeks bij DPO ingediend worden (bv., recht op inzage, verwijdering, …)
- Bijhouden en actualiseren lijst veelgestelde vragen + antwoorden

[3] art. 35 AVG: Indien 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 vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.

2.3.1.5. Risico's signaleren aan afgevaardigd bestuurder en suggesties doen voor passende risicobeperkende maatregelen

- Op geregelde tijdstippen verslag uitbrengen bij de Afgevaardigd Bestuurder, Algemeen Directeurs en aanspreekpunten aangaande gegevenslekken en voorstel van maatregelen

2.3.1.6. Samenwerken met de toezichthoudende autoriteiten en optreden als aanspreekpunt voor deze autoriteiten

- Gegevensbeschermingsautoriteit (afgekort GBA, federale instelling)
- Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens (afgekort VTC)

2.3.1.7. Externe vertegenwoordiging op beleidsvoorbereidend domein

- Overleg met DPO's onderwijskoepels, Departement Onderwijs en Gegevensbeschermingsautoriteit (GBA) en Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens (VTC)
- Kennisuitwisseling

2.3.1.8. Agenderen/aanleveren voorstel agenda CORA en STAP

2.3.2. Raad van het GO!

2.3.2.1. Beslissen over de beleidsmaatregelen binnen het GO!

- Voorbereiding gebeurt door DPO

2.3.3. Afgevaardigd bestuurder

2.3.3.1. Kennis nemen van gesignaleerde risico's en de voorgestelde passende maatregelen ter beperking van deze risico's en hierover beslissen

- Signaleren van de risico's gebeurt door data protection officer

2.3.4. Personeelsleden van de centrale diensten

2.3.4.1. Naleven richtlijnen aangaande informatieveiligheid
2.3.4.2. Meldplicht informatieveiligheidsincidenten en gegevenslekken

2.4. Niveau overstijgend

2.4.1. Informatieveiligheidscel GO!

- Op elkaar afstemmen van beleidsvraagstukken over de verschillende niveaus

3. Procedures

3.1. Wat te doen bij een beveiligingsincident / gegevenslek?

3.1.1. Wat is een beveiligingsincident?

Een beveiligingsincident is **elke ongewenste en/of onverwachte gebeurtenis met een betekenisvolle of mogelijke impact op de informatieveiligheid** (beschikbaarheid, integriteit, vertrouwelijkheid en onweerlegbaarheid van informatie en -systemen).

Er is sprake van een informatieveiligheidsincident van zodra sprake is van een betekenisvolle of mogelijke impact op één van de volgende 4 aspecten van informatieveiligheid:

- **Vertrouwelijkheid** of confidentialiteit: een informatie-eigenschap waardoor alleen gemachtigde personen, entiteiten of processen toegang hebben tot informatie en waardoor informatie alleen kan worden doorgegeven aan gemachtigde personen, entiteiten of processen.

- **Integriteit**: het waarborgen van de correctheid en de volledigheid van de informatieverwerking. De integriteit van informatie is de eigenschap waardoor die informatie niet opzettelijk of onopzettelijk kan worden veranderd of vernietigd. De integriteit van een systeem of proces is de eigenschap om de gewenste functie volledig en volgens de verwachtingen te verwezenlijken, waarbij het zonder een gemachtigde tussenkomst niet mogelijk is opzettelijke of onopzettelijke veranderingen aan te brengen.

- **Authenticiteit**: het moet ondubbelzinnig vaststaan van wie de informatie is (komt). Onder authenticiteit wordt verstaan dat een entiteit diegene is die ze beweert te zijn. Authenticiteit wordt toegepast op personen (gebruikers) maar ook op elke andere entiteit (applicatie, processen, systeem, enz.). Het is een identificatie, d.w.z. een herkenning van een benaming waardoor een entiteit zonder enige twijfel kan worden aangewezen.

- **Beschikbaarheid** betekent dat informatie(systemen) toegankelijk en bruikbaar zijn op de juiste momenten op verzoek van een gemachtigde entiteit.

- **Onweerlegbaarheid:** betekent dat een bewerking of gebeurtenis daadwerkelijk plaatsvond en niet nu noch later ontkend kan worden.

3.1.2. Wat is een gegevenslek?

Een gegevenslek is een inbreuk op de beveiliging 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 persoonsgegevens.

Een gegevenslek is dus **een beveiligingsincident waarbij persoonsgegevens gecompromitteerd werden** (ongeoorloofde inzage, publicatie, verlies, vernietiging, wijziging). Het speelt daarbij geen rol op welke wijze de persoonsgegevens zijn opgeslagen (digitaal, papier, …), noch of er sprake is van opzet, dan wel een ongeluk.

Het begrip gegevensinbreuk is dus zeer ruim. Essentieel element in de beoordeling is de vraag of persoonsgegevens zijn gecompromitteerd.

Voorbeelden van gegevenslekken:

- Het hacken van de netwerkomgeving.
  Als een organisatie voor de beveiliging van de systemen een verouderde versie van antivirussoftware gebruikt, is er nog geen sprake van een datalek, wel van een beveiligingsincident. Maar zodra als gevolg van een virusbesmetting de systemen waarop zich persoonsgegevens bevinden toegankelijk zijn geworden voor derden, is er wel sprake van een gegevenslek.
- De diefstal van een boekentas met daarin verslagen van een CLB-medewerker.
- Het verlies van een USB-stick van een leraar met daarop leerlingenbeoordelingen.
- Een map met sollicitatiebrieven en cv's wordt per ongeluk meegegeven met het oud papier.

3.1.3. Verplichtingen bij beveiligingsincident / gegevenslek

3.1.3.1. Registreren in het incidentenregister

Elk beveiligingsincident moet gedocumenteerd worden in een incidentenregister, waarbij een analyse moet gemaakt worden van het incident en moet worden bijgehouden welke maatregelen worden genomen om dergelijk incident in de toekomst te vermijden[4]. Die documentatie stelt de bevoegde autoriteit voor gegevensbescherming in staat de naleving van de meldplicht te controleren.

Het incidentenregister bevat minstens:

- De (vermoedelijke) datum van de inbreuk
- De aard van de inbreuk
- De oorzaak van de inbreuk
- Frequentie van de inbreuk
- Een omschrijving van de mogelijke gevolgen
- Een omschrijving van de maatregelen die werden genomen om dergelijke inbreuk in de toekomst te vermijden
- Een omschrijving van de maatregelen die werden genomen om de nadelige gevolgen van de inbreuk te verminderen
- Deze informatie is opgenomen in tabel 2 van het meldingsformulier beveiligingsincident.
- De opname in een incidentenregister staat los van de eventuele melding aan de bevoegde autoriteit en dient dus ook te gebeuren als zo'n melding niet nodig is, omdat er geen persoonsgegevens werden gecompromitteerd of het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten van betrokkenen

3.1.3.2. Melden bij de Vlaamse Toezichtcommissie

Elk gegevenslek (dus steeds wanneer persoonsgegevens gecompromitteerd worden) **moet worden gemeld** bij de bevoegde autoriteit, **tenzij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van de betrokkene** (o.a. en voornamelijk het recht op bescherming van de persoonlijke levenssfeer).[5] Deze melding moet zo snel mogelijk gebeuren en uiterlijk binnen de 72 uur (3 dagen) na kennisname van het gegevenslek gebeuren. In het geval van vertraging moet hiervoor een specifieke motivering worden meegegeven.

De autoriteit bevoegd om meldingen in ontvangst te nemen van het GO! is de Vlaamse Toezichtcommissie voor de bescherming van persoonsgegevens (http://vtc.corve.be/).

[4] art. 33 5° AVG.
[5] Art. 33 AVG.

Daarnaast dient de verwerkingsverantwoordelijke tevens alle inbreuken te documenteren, met inbegrip van de feitelijke context van de inbreuk, de gevolgen ervan en de genomen corrigerende maatregelen.

In de melding wordt ten minste het volgende meegedeeld:

- De aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en type persoonsgegevens in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevens in kwestie
- De naam en de contactgegevens van de data protection officer en het aanspreekpunt voor informatieveiligheid, waar meer informatie kan worden verkregen
- De waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens
- De maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan
- De te verstrekken informatie is opgenomen in tabel 3 van het meldingsformulier beveiligingsincident

Indien het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie in stappen worden verstrekt (echter zonder onredelijke vertraging).

Indien een inbreuk door een verwerker (bv. softwareleverancier) wordt vastgesteld moet deze de verwerkingsverantwoordelijke informeren van zodra hij kennis heeft genomen van de inbreuk. De verwerkingsverantwoordelijke moet vervolgens zelf de Gegevensbeschermingsautoriteit / betrokkene informeren zoals hierboven beschreven. De modaliteiten daarvan moeten vastgelegd worden in de overeenkomst die met deze verwerker wordt afgesloten.

3.1.3.3. Betrokkenen in kennis stellen van het gegevenslek

Wanneer een gegevenslek waarschijnlijk een risico inhoudt voor de rechten en vrijheden van betrokkenen (inbegrepen het recht op privacy), moeten de betrokkenen daarvan worden in kennis gesteld.

Uitzondering: Deze kennisgeving moet evenwel niet gebeuren indien op de gelekte persoonsgegevens passende technische en organisatorische beschermingsmaatregelen werden genomen waardoor deze onbegrijpelijk zijn gemaakt voor onbevoegden (bijvoorbeeld encryptie), of wanneer na het gegevenslek maatregelen werden genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen.

De te verstrekken informatie om na te gaan of al dan niet een kennisgeving aan de betrokkenen moet gebeuren is opgenomen in tabel 3.2 van het meldingsformulier beveiligingsincident.

3.1.4. Wie moet instaan voor melding, registratie en kennisgeving?

3.1.4.1. Elk personeelslid heeft een meldingsplicht

Elk personeelslid dat kennis krijgt van een informatieveiligheidsincident of een gegevenslek, of daar door derden op wordt gewezen, dient dat naargelang de aard van de instelling waar het beveiligingsincident zich voordoet onmiddellijk te melden aan de directeur van de instelling, het aanspreekpunt informatieveiligheid of de data protection officer.

Een personeelslid van een lokale instelling dient dit te melden aan zijn/haar directeur.
Een personeelslid van een scholengroep dient dit te melden aan het aanspreekpunt informatieveiligheid.

Een personeelslid van de centrale diensten dient dit te melden aan de data protection officer.

3.1.4.2. Directeur van een lokale instelling

Op het lokale niveau staat **de directeur** in voor het actualiseren en bijhouden van het register van de incidenten die betrekking hebben op zijn/haar instelling. Het incidentenregister en het register van de verwerkingen van persoonsgegevens moeten te allen tijde actueel worden gehouden in de IVOS-tool waar de algemeen directeur en het aanspreekpunt informatieveiligheid ze kunnen raadplegen.

3.1.4.3. Het aanspreekpunt informatieveiligheid

Op het mesoniveau staat het **aanspreekpunt informatieveiligheid** in voor het actualiseren en bijhouden van het register van de incidenten die betrekking hebben op zijn/haar scholengroep. De directeurs van de instellingen van het lokale niveau zijn gehouden het aanspreekpunt informatieveiligheid bij het vervullen van deze taak bij te staan. Het incidentenregister en het register van de verwerkingen van persoonsgegevens moeten te allen tijde actueel worden gehouden in de IVOS-tool waar de algemeen directeur en het aanspreekpunt informatieveiligheid ze kunnen raadplegen.

Het aanspreekpunt informatieveiligheid handelt evenwel als gedelegeerde van de **algemeen directeur**, die de eindverantwoordelijkheid draagt.

3.1.4.4. Data protection officer en informatieveiligheidsconsulent

Op het centrale niveau staan de **data protection officer** en **Informatieveiligheidsconsulent** in voor het actualiseren en bijhouden van het register van de incidenten die betrekking hebben op het centrale niveau. De incidentenregisters en de registers van de verwerkingen van persoonsgegevens van het centrale niveau, de tussenniveaus en de lokale niveaus moeten door de data protection officer worden ter beschikking worden gesteld van de Gegevensbeschermingsautoriteit wanneer deze erom verzoekt.

3.1.5. Interne procedure voor afhandeling beveiligingsinbreuk

De afhandeling van de procedure verloopt in 6 van elkaar te onderscheiden stappen:

1. Ontdekking en interne melding
2. Beoordeling
3. Registratie
4. Remediëring
5. Melding bij de Vlaamse Toezichtcommissie
6. Kennisgeving aan de betrokkene

3.1.5.1. Ontdekking en interne melding

Een personeelslid dat zelf een beveiligingsincident ontdekt, of daar door derden op wordt gewezen, dient dat, naargelang de aard van de instelling waar het incident zich voordoet, onverwijld te melden aan zijn/haar directeur, het aanspreekpunt voor informatieveiligheid of zijn afdelingshoofd.

Een personeelslid van een lokale instelling dient dit te melden aan zijn/haar directeur.
Een personeelslid van een scholengroep dient dit te melden aan het aanspreekpunt informatieveiligheid.
Een personeelslid van de centrale diensten dient dit te melden aan zijn/haar afdelingshoofd en de data protection officer.

De melding gebeurt bij voorkeur schriftelijk en meteen na de ontdekking van het beveiligingsincident.

3.1.5.2. Beoordeling

Wanneer de directeur/het aanspreekpunt/de data protection officer worden in kennis gesteld van een beveiligingsinbreuk gaat deze na of hij over voldoende informatie beschikt om de draagwijdte van de inbreuk na te gaan. Hij kan andere personeelsleden bevragen om hem de informatie te bezorgen die hij ontbreekt. De directeur/het aanspreekpunt/de data protection officer beoordeelt op basis van de feiten of het gaat om een loutere beveiligingsinbreuk, een gegevenslek, en of het al dan niet nodig is om betrokkenen op de hoogte te brengen.

Het invullen van het meldingsformulier en de ja/nee vragen die erin opgenomen zijn fungeren als leidraad bij de beoordeling of er al dan niet moet worden gemeld aan de VTC en of de betrokkenen moeten worden in kennis gesteld.

3.1.5.3. Registratie beveiligingsinbreuk

De directeur van een lokale instelling, aanspreekpunt informatieveiligheid of data protection officer die kennis krijgt van een beveiligingsincident staat in voor de registratie van dat beveiligingsincident in het register van beveiligingsincidenten.

Dit gebeurt binnen een sjabloon aangeleverd door de centrale diensten, in de vorm van daartoe ontwikkelde software.

Bij de registratie dient zo veel mogelijk relevante informatie te worden gevoegd die moet toestaan de risico's te beoordelen. De informatie die aan de melding wordt toegevoegd, moet aangereikt worden door de instelling(en) waar het lek zich heeft voorgedaan.

In elk geval moet aangaande de aard van de beveiligingsinbreuk een antwoord op de volgende vragen te worden gegeven.

Informatie aangaande de beveiligingsinbreuk
Is er sprake van een ongewenste en/of onverwachte gebeurtenis met een betekenisvolle of mogelijke impact op de beschikbaarheid, integriteit, vertrouwelijkheid of onweerlegbaarheid van informatie? [6]
Wat is de aard van de inbreuk?
Wat is de oorzaak van de inbreuk?
Datum waarop de inbreuk (vermoedelijk) is gebeurd
Frequentie van de inbreuk(en)
Wat zijn de waarschijnlijke gevolgen van de inbreuk?

3.1.5.4. Remediëren beveiligingsincident

De directeur van een lokale instelling, aanspreekpunt informatieveiligheid of data protection officer die kennis krijgt van een beveiligingsincident, overlegt met de daartoe bevoegde technici (intern of extern) om te achterhalen wat de oorzaak van het beveiligingsincident is en welke technische en organisatorische maatregelen dienen te worden genomen om de oorzaak van de beveiligingsinbreuk aan te pakken.

De voorgenomen remediërende maatregelen dienen eveneens geregistreerd te worden.

[6] Enkel indien het antwoord op deze vraag 'ja' is gaat het over een beveiligingsincident en moet tot registratie worden overgegaan.

Remediërende maatregelen
Welke maatregelen werden voorgesteld of genomen om (de oorzaak van) de beveiligingsinbreuk aan te pakken?

De registratie moet aan de toekomstige maatregelen een einddatum koppelen en de directeur van een lokale instelling, aanspreekpunt informatieveiligheid of data protection officer staan in voor opvolging en monitoring van de te nemen maatregelen.

Niveau incident	Verantwoordelijk voor registratie en opvolging
Lokale instelling	Directeur
Scholengroep	Aanspreekpunt informatieveiligheid
Centrale diensten	Data protection officer

Tenzij wanneer de beveiligingsinbreuk ook als een gegevenslek moet gekwalificeerd worden[7], is de beveiligingsinbreuk afgehandeld indien bovenvermelde informatie werd geregistreerd en de verantwoordelijke instaat voor opvolging en monitoring van de te nemen maatregelen.

Bij registratie dient elke beveiligingsinbreuk een logisch nummer te krijgen, dat wordt vermeld in het register.

3.1.5.5. Melding aan de Vlaamse Toezichtcommissie

Indien de beveiligingsinbreuk heeft geleid tot een onbedoelde of onrechtmatige vernietiging, verlies, wijziging, ongeoorloofde verstrekking of ongeoorloofde toegang tot persoonsgegevens is er sprake van een gegevenslek. In dat geval moet, naast de registratie voor intern gebruik, ook een melding gebeuren aan de Vlaamse Toezichtcommissie.

De melding aan de Vlaamse Toezichtcommissie dient naast de verplicht te registreren gegevens minstens de volgende informatie bevatten aangaande het gegevenslek:

3.1 Informatie aangaande het gegevenslek	
Heeft de inbreuk geleid tot een onbedoelde of onrechtmatige vernietiging, verlies, wijziging, ongeoorloofde verstrekking of ongeoorloofde toegang tot persoonsgegevens ? + motiveer je antwoord	*Ja / nee*[8] *Indien het antwoord op deze vraag nee is moet de rest van de tabel niet ingevuld worden*
Wat is het doel van de verwerking van de persoonsgegevens?	

[7] Dat is wanneer de inbreuk heeft geleid tot een onbedoelde of onrechtmatige vernietiging, verlies, wijziging, ongeoorloofde verstrekking of ongeoorloofde toegang tot persoonsgegevens.

[8] Indien ja: het gaat om een gegevenslek, het volledige formulier moet ingevuld worden om na te gaan welke bijkomende actie vereist is: indien nee-> het gaat niet om een gegevenslek, maar uitsluitend over een beveiligingsinbreuk.

Geef aan welke categorieën persoonsgegevens betrokken zijn (vb: financiële gegevens)	☐ *Identificatiegegevens* ☐ *Gezinssamenstelling* ☐ *Schoolloopbaan leerlingen* ☐ *Studiebewijzen leerlingen* ☐ *Beroepsloopbaan personeel* ☐ *Contactgegevens* ☐ *Arbeidsongevallen* ☐ *Uitgaven waarvoor terugbetaling wordt gevraagd* ☐ *Diplomagegevens personeel* ☐ *Rijksregisternummer* ☐ *Wachtwoord* ☐ *Ter beschikking gestelde IT-middelen* ☐ *Historiek verrichtingen met IT-middelen* ☐ *Elektronische localisatiegegevens* ☐ *Foto's* ☐ *Video-, beeld- en geluidsopnames* ☐ *Bankrekeningnummer* ☐ *Nummer debetkaart* ☐ *Nummer kredietkaart* ☐ *Beslag door derden/solvabiliteit* ☐ *Gezondheidsgegevens* ☐ *Psychologisch profiel* ☐ *Biometrische identificatiegegevens* ☐ *Leefgewoonten* ☐ *Fysieke beschrijving* ☐ *Politieke overtuiging* ☐ *Lidmaatschap van een vakbond* ☐ *Raciale of etnische gegevens* ☐ *Filosofische of religieuze overtuiging* ☐ *Gegevens betreffende het seksuele leven* ☐ *Gerechtelijke gegevens*
Geef aan welke categorieën personen betrokken zijn (vb: leerlingen 1ste graad)	☐ Leerlingen ☐ Ouder(s)/opvoedingsverantwoordelijke(n) ☐ Personeel ☐ Klanten ☐ Leveranciers/ Aannemers ☐ Gastdocenten ☐ Stagiairs ☐ Sollicitanten ☐ Potentiële leveranciers/aannemers ☐ Andere, specifieer:
Geef het aantal betrokkenen (desnoods bij benadering)	
Zijn er verwerkers of andere derden betrokken bij het gegevenslek?	☐ Nee ☐ Ja, welke?:

Wat zijn de waarschijnlijke gevolgen van het gegevenslek ?	
Hoe hoog is het risico voor de rechten en vrijheden (inclusief recht op privacy) van betrokkenen? Eventuele opmerking:	☐kritisch ☐hoog ☐medium ☐laag ☐verwaarloosbaar ☐nog niet bepaald Klik of tik om tekst in te voeren.

Tips/richtlijnen bij het inschatten van het risico:

Verwaarloosbaar risico	*Betrokkenen zullen een slechts uiterst beperkte impact ondervinden. (bvb. e-mailadres is openbaar)*
Laag risico	*Betrokkenen zullen een matige impact ondervinden (bvb. tijd besteden aan het opnieuw invoeren van informatie, ergernissen, irritaties, etc.)*
Medium risico	*Betrokkenen zullen aanzienlijke impact ondervinden (bvb. extra kosten, ontzegging van toegang tot zakelijke diensten, angst, gebrek aan begrip, stress, enz.)*
Hoog risico	*Betrokkenen zullen een significante impact ondervinden (bvb. ontvreemding van (geld)middelen, op zwarte lijsten bij banken en/of verzekeringsmaatschappijen , materiële schade, verlies van werk, dagvaarding, verslechtering van de gezondheid, enz.)*
Kritisch risico	*Betrokkenen zullen een significante of zelfs onomkeerbare impact/gevolgen ondervinden (bvb. zware discriminatie, financiële nood, arbeidsongeschiktheid, langdurige psychische of fysieke kwalen, enz.)*

- **Bijlagen**: stuur indien mogelijk **bijlagen** door (bv. in de vorm van screenshots)

Wanneer er sprake is van een gegevenslek moet bij de melding tevens worden aan de melding toegevoegd welke maatregelen genomen ter beperking van de eventuele nadelige gevolgen voor de betrokkene(n). (bijvoorbeeld onleesbaar maken gegevens door encryptie). Ook deze informatie moet toegevoegd worden aan de melding bij de VTC.

Hieronder handelen de onderstaande vragen die eveneens werden opgenomen in het aangifteformulier:

Werden passende technische en organisatorische beschermingsmaatregelen genomen waardoor de gelekte persoonsgegevens onbegrijpelijk zijn gemaakt voor onbevoegden? Zo ja, welke ?	*Ja / nee* [9]
Werden na het gegevenslek maatregelen genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen? Zo ja, welke ?	*Ja / nee* [10]
Is logging beschikbaar	☐ Nee ☐ Ja
Zijn de betrokkenen geïnformeerd?	☐ Ja Datum: ☐ Nee, nog niet Geplande datum: ☐ Nee: Reden: Via welk communicatiemiddel? ☐ Brief ☐ Mail ☐ Andere:
Zou mededeling aan de betrokkenen onevenredige inspanningen vergen?	*Ja / nee* [11]

Afhandeling van de melding voor een gegevenslek op het niveau van een lokale instelling

Voor gegevenslekken op het lokale niveau staat **de directeur** in voor het voorbereiden van de melding aan het VTC door alle informatie waarover hij reeds beschikt in te vullen op het meldingsformulier of de daarvoor ontwikkelde tool.

Hij maakt deze informatie over aan het aanspreekpunt informatieveiligheid van de scholengroep, die nagaat of de informatie zijns inziens volledig is.

De directeur en de personeelsleden van de lokale instelling die weet hebben van de omstandigheden van het gegevenslek houden zich ter beschikking van het **aanspreekpunt informatieveiligheid** voor

[9] Indien ja -> betrokkene moet niet worden in kennis gesteld ; indien nee -> betrokkene moet worden in kennis gesteld
[10] Indien ja -> betrokkene moet niet worden in kennis gesteld ; indien nee -> betrokkene moet worden in kennis gesteld
[11] Indien ja -> kennisgeving aan betrokkene moet vervangen worden door een openbare mededeling of een soortgelijke maatregel; indien nee -> betrokkene moet worden in kennis gesteld

het geval deze nog aanvullende informatie nodig heeft, en geven maximale medewerking bij het verzamelen van de informatie en de verdere afhandeling van de procedure.

Het aanspreekpunt informatieveiligheid van de scholengroep maakt de melding over aan de **data protection officer**, die vervolgens eveneens nagaat of de informatie zijns inziens volledig is.

Het aanspreekpunt informatieveiligheid, de directeur en de personeelsleden van de lokale instelling die weet hebben van de omstandigheden van het gegevenslek houden zich ter beschikking van de data protection officer voor het geval deze nog aanvullende informatie nodig heeft, en geven maximale medewerking bij de verdere afhandeling van de procedure.

Van zodra de data protection officer van oordeel is dat de nodige informatie voorhanden is, gaat hij over tot het indienen van de melding bij de Vlaamse Toezichtcommissie. Hij geeft het aanspreekpunt informatieveiligheid en de directeur verder ook advies over de afhandeling en opvolging van de voorgenomen remediërende maatregelen en eventuele kennisgeving aan de betrokkenen.

Uitzondering: Wanneer omwille van tijdsgebrek geen nuttig overleg tussen het aanspreekpunt en de centrale diensten meer kan georganiseerd worden dient het aanspreekpunt informatieveiligheid zelf over te gaan tot melding aan de Gegevensbeschermingsautoriteit, opdat de melding binnen de 72 uur na vaststelling van het gegevenslek zou gebeuren. De melding gebeurt per e-mail op het e-mailadres toezichtcommissie@vlaanderen.be en moet als mededeling vermelden, “melden gegevenslek”, gevolgd door naam van de instelling. Hierbij moet aangegeven worden dat het gaat om een voorlopige melding, en dat de ontbrekende informatie zo snel mogelijk zal toegevoegd worden.

Afhandeling van de melding bij gegevenslek op het niveau van een scholengroep

Voor gegevenslekken op het niveau van een scholengroep staat het **aanspreekpunt informatieveiligheid** in voor het voorbereiden van de melding aan het VTC door alle informatie waarover hij reeds beschikt in te vullen op het meldingsformulier of de daarvoor ontwikkelde tool.

De personeelsleden van de scholengroep die weet hebben van de omstandigheden van het gegevenslek houden zich ter beschikking van het **aanspreekpunt informatieveiligheid** voor het geval deze aanvullende informatie nodig heeft, en geven maximale medewerking bij het verzamelen van de informatie en de verdere afhandeling van de procedure.

Het aanspreekpunt informatieveiligheid van de scholengroep maakt de melding over aan de **data protection officer**, die vervolgens nagaat of de informatie zijns inziens volledig is.

Het aanspreekpunt informatieveiligheid en de personeelsleden van de scholengroep die weet hebben van de omstandigheden van het gegevenslek houden zich ter beschikking van de data protection officer voor het geval deze nog aanvullende informatie nodig heeft, en geven maximale medewerking bij de verdere afhandeling van de procedure.

Van zodra de data protection officer van oordeel is dat de nodige informatie voorhanden is gaat hij over tot het indienen van de melding bij de Vlaamse Toezichtcommissie. Hij geeft het aanspreekpunt informatieveiligheid verder ook advies over de afhandeling en opvolging van de voorgenomen remediërende maatregelen en eventuele kennisgeving aan de betrokkenen.

Uitzondering: Wanneer omwille van tijdsgebrek geen nuttig overleg tussen het aanspreekpunt en de centrale diensten meer kan georganiseerd worden dient het aanspreekpunt informatieveiligheid zelf over te gaan tot melding aan de Gegevensbeschermingsautoriteit, opdat de melding binnen de 72 uur na vaststelling van het gegevenslek zou gebeuren. De melding gebeurt per e-mail op het e-mailadres toezichtcommissie@vlaanderen.be en moet als mededeling vermelden, “melden gegevenslek”, gevolgd door nummer en naam van de scholengroep. Hierbij moet aangegeven worden dat het gaat

om een voorlopige melding, en dat de ontbrekende informatie zo snel mogelijk zal toegevoegd worden.

Afhandeling van een gegevenslek op het niveau van de centrale diensten / het volledige GO

Het personeelslid van de centrale diensten dat een gegevenslek vaststelt, of erop gewezen wordt, dient dat te melden aan zijn afdelingshoofd en aan de DPO. Dit gebeurt via de knop 'Meldpunt' op de homepagina.

De personeelsleden die weet hebben van de omstandigheden van het gegevenslek houden zich ter beschikking van de DPO en afdeling IT voor het geval deze aanvullende informatie nodig heeft, en geven maximale medewerking bij het verzamelen van de informatie en de verdere afhandeling van de procedure.

3.1.5.6. Informeren betrokkene(n)

Indien het gegevenslek waarschijnlijk ongunstige gevolgen met zich me kan brengen voor de rechten en vrijheden (o.a. het recht op bescherming van de persoonlijke levenssfeer) **van de betrokkene**, dan moet het gegevenslek ook aan de betrokkenen zelf worden gemeld. Dat zijn medewerkers, leerlingen of hun ouders, als zij jonger zijn dan 16 jaar.

Als stelregel dient men ervan uit te gaan dat wanneer persoonsgegevens van gevoelige aard zijn gelekt het risico voor ongunstige gevolgen voor de privacy van betrokkenen inderdaad waarschijnlijk is. Denk daarbij bijvoorbeeld aan een afdruk uit het leerlingenvolgsysteem met beschrijving pestgedrag of onderzoeksresultaten CLB.

Een melding aan de betrokkene(n) moet niet gebeuren wanneer de gelekte persoonsgegevens zijn beveiligd of versleuteld, en de gelekte data onbegrijpelijk of ontoegankelijk zijn voor derden. Denk daarbij bijvoorbeeld aan het lekken van een beveiligde én versleutelde database met persoonsgegevens.

Indien de betrokkene(n) worden geïnformeerd dient dit ook aan de melding bij de VTC te worden toegevoegd.

3.2. Wat te doen als een betrokkene zijn rechten wil laten gelden?

3.2.1. Wat is een betrokkene?

De AVG omschrijft persoonsgegevens als alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, 'de betrokkene'.

De **betrokkene** is dus een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van identificatie-gegevens zoals een naam, een identificatienummer, locatiegegevens, een ip-adres of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

In onderwijscontext worden alvast zeker persoonsgegevens verwerkt van leerlingen/cursisten en personeelsleden. Er zullen evenwel ook gegevens worden verwerkt van leveranciers of bezoekers.

3.2.2. Welke rechten kan een betrokkene laten gelden?

3.2.2.1. Recht op transparantie

De verwerkingsverantwoordelijke is ertoe gehouden om de betrokkene in een begrijpelijke taal mede te delen welke persoonsgegevens hij verwerkt, met welk doel hij dat doet, en wat daarvoor de rechtsgrond is. Daarnaast dienen ook contactgegevens van de DPO worden medegedeeld, en moet worden medegedeeld of persoonsgegevens aan derden worden medegedeeld. Deze informatie wordt het best opgenomen in een privacyverklaring.

Deze privacyverklaring kan toegevoegd worden aan het schoolreglement en wordt best ook gepubliceerd op de website. De verwerkingsverantwoordelijke dient deze informatie zelf spontaan te publiceren, dus zonder dat de betrokkene daarom vraagt.

3.2.2.2. Recht op inzage in de persoonsgegevens

De betrokkene heeft het recht om uitsluitsel te krijgen over de vraag of zijn persoonsgegevens als of niet worden verwerkt, en om in het laatste geval inzage te krijgen van die persoonsgegevens en van de volgende informatie:

a) De verwerkingsdoeleinden;
b) De categorieën van persoonsgegevens die worden verwerkt;
c) De ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
d) Indien mogelijk, de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
e) Dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken dat persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van hem betreffende persoonsgegevens wordt beperkt, alsmede het recht tegen die verwerking bezwaar te maken;
f) Dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit;
g) Wanneer de persoonsgegevens niet bij de betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens;
h) Het bestaan van geautomatiseerde besluitvorming indien dat het geval is.

3.2.2.3. Recht op verbetering van de persoonsgegevens

De betrokkene heeft het recht om onverwijld verbetering van hem betreffende onjuiste persoonsgegevens te verkrijgen.

3.2.2.4. Recht op wissen ('recht om vergeten te worden')

Betrokkenen hebben het recht binnen redelijke termijn van de verwerkingsverantwoordelijke te eisen dat de hem betreffende persoonsgegevens worden gewist.

Belangrijke bedenking daarbij is dat de verwerkingsverantwoordelijke wel verplicht is om deze vraag te behandelen en te beantwoorden, maar dat hij slechts in een beperkt aantal gevallen ook daadwerkelijk verplicht is om de gegevens te verwijderen.

De verwerkingsverantwoordelijke is verplicht tot wissen in de volgende gevallen:

- De persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld
- De betrokkene trekt de toestemming in waarop de verwerking berust
- De persoonsgegevens zijn onrechtmatig verwerkt
- Er is een wettelijke verplichting tot wissen

De meerderheid van de verwerkingen binnen het GO! zal gebeuren op basis van wettelijke verplichtingen. Zolang de persoonsgegevens nog noodzakelijk zijn voor het voldoen aan de wettelijke verplichtingen dient uiteraard niet te worden ingegaan op een verzoek tot wissen. Wel moet in voorkomend geval op dit verzoek op een gemotiveerde wijze worden geantwoord waarom de gegevens niet zullen gewist worden.

3.2.3. Procedure voor uitoefening rechten door een betrokkene

3.2.3.1. Indienen van het verzoek

Afhankelijk van het geval zullen vragen tot uitoefening van hun rechten door betrokkenen worden gesteld aan de directeur, het aanspreekpunt informatieveiligheid of de data protection officer.

Indien dergelijke vraag aan andere personeelsleden zou worden gesteld dienen zij deze vraag onverwijld door te sturen naar de directeur, het aanspreekpunt informatieveiligheid of de data protection officer.

De betrokkenen dienen de vraag tot uitoefening van hun rechten schriftelijk te stellen, bij voorkeur per e-mail. Mondelinge of telefonische vragen zullen niet worden behandeld. Betrokkenen die mondeling of telefonisch dergelijke vraag stellen, dienen te worden doorverwezen naar het personeelslid dat gemachtigd is om deze verzoeken af te handelen.

3.2.3.2. Identificatie van de betrokkene

Wanneer een betrokkene een vraag stelt tot uitoefening van het recht op inzage, wissen of verbeteren van persoonsgegevens dient in eerste instantie te worden nagegaan of deze vraag wel uitgaat van de persoon die zich uitgeeft voor de betrokkene. Van zodra twijfel mogelijk is of de vraag wel uitgaat van de betrokkene moet de identiteit van de vraagsteller worden gecontroleerd. Dit is dus niet nodig indien het duidelijk is dat de vraag niet door iemand anders wordt gesteld (bv., de betrokkene biedt zich zelf persoonlijk aan bij de directeur, de vraag wordt per mail gesteld vanop hetzelfde e-mail adres dat in de bestanden zit, …).

De vraagsteller dient bij twijfel over zijn identiteit dus te worden gevraagd om zich te identificeren aan de hand van zijn identiteitskaart of een gelijkaardig document. Een kopie of scan van de voor- en achterzijde

van dat identiteitsdocument dienen te worden overgemaakt om die identificatie mogelijk te maken. Identiteitsdocumenten waarvan de geldigheidsduur is verstreken zullen niet worden aanvaard.

Als de identiteit van een vraagsteller niet kan worden bewezen aan de hand van een geldig identiteitsdocument mag geen gevolg worden gegeven aan zijn verzoek. Er kan een antwoord worden gestuurd met volgende tekst:

Beste,

Wij nemen de privacy van onze leerlingen, personeelsleden en derden zeer ernstig en kunnen pas op uw verzoek ingaan na behoorlijke controle van uw identiteit. Dit betekent dat wij absoluut willen vermijden inzage te geven in gegevens van onze leerlingen- of personeelsleden aan onbevoegde derden.

Ik verzoek u dan ook om mij een scan of kopie van de voor- en achterzijde van uw identiteitskaart te bezorgen, zodat ik de ontvankelijkheid van uw vraag kan onderzoeken.

Met vriendelijke groeten,

Pas na mededeling van geldige identiteitsdocumenten, en nadat blijkt dat de vraag ook daadwerkelijk uitgaat van de betrokkene, kan de afhandeling van het verzoek worden verder gezet.

3.2.3.3. Beoordeling van het verzoek

Verzoek tot inzage

Van zodra de betrokkene behoorlijk is geïdentificeerd kan zijn verzoek worden beoordeeld. Een **verzoek tot inzage** dient steeds te worden toegestaan. Dit kan aan de hand van de volgende modelbrief:

Beste,

U vindt in de bijgevoegde tabel een overzicht van uw door ons verwerkte persoonsgegevens en de informatie die wij u in toepassing van de Algemene Verordening Gegevensbescherming moeten verschaffen.

U heeft het recht om ons te verzoeken dat deze persoonsgegevens worden verbeterd of gewist, om te vragen om de verwerking te beperken en in bepaalde omstandigheden ook om bezwaar te maken tegen de verwerking. Deze vragen kan u stellen via het e-mail adres dpo@g-o.be.
Indien u klachten heeft tegen de wijze waarop uw persoonsgegevens worden verwerkt kan u dit doen bij de Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens, die u terugvindt op de website www.vtc.corve.be.

Met vriendelijke groeten,

De tabel die aan deze brief moet worden toegevoegd, moet alle persoonsgegevens van de betrokkene bevatten waarover het GO! beschikt, evenals de volgende informatie:

- De verwerkingsdoeleinden

- De betrokken categorieën van persoonsgegevens
- De ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt
- De periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen, of de criteria om die termijn te bepalen
- Het bestaan van geautomatiseerde besluitvorming indien dat het geval is (hetgeen in de context van het GO! zeer onwaarschijnlijk is)

Verzoek tot verbetering

Een **verzoek tot verbetering** van gegevens dient eveneens te worden uitgevoerd, doch na controle van de juistheid van de gegevens, desnoods na voorlegging van stukken. Een verzoek tot verbetering moet van zodra de juistheid van de gevraagde verbetering onverwijld worden uitgevoerd.

Verzoek tot wissen, tot beperking van de verwerking of een bezwaar tegen de verwerking

Een **verzoek tot wissen, een verzoek tot beperking van de verwerking of een bezwaar tegen de verwerking** kan alleen worden uitgevoerd in zeer specifieke omstandigheden. Afhankelijk van de rechtsgrond waarop de verwerking is gebaseerd zijn er ook heel wat gevallen waarin op zo'n verzoek niet mag of kan ingegaan worden.

Op dergelijke verzoeken kan dus alleen worden ingegaan na het inwinnen van het advies van de data protection officer. Dit advies zal worden geformuleerd aan de hand van het register van de verwerkingen en de verwerkingsdoeleinden en rechtsgronden voor de verwerking die daar zijn geïdentificeerd.

3.2.3.4. Termijnen

Verzoeken van de betrokkene tot uitoefening van hun rechten dienen zo snel mogelijk ('onverwijld') te worden afgehandeld, zonder dat de vertraging meer dan **een maand** mag bedragen.

In het geval van een complexe vraag die niet binnen de maand kan worden afgehandeld kan die termijn nog eens **met twee maanden worden verlengd**. Dit dient evenwel binnen de maand na initiële aanvraag schriftelijk aan de betrokkene te worden gemeld.

De betrokkene moet schriftelijk geïnformeerd worden van zodra de voorgenomen actie werd voltooid, en van het geplande nazicht.

3.2.3.5. Nazicht van het effectief karakter van de genomen actie.

Indien wordt ingegaan op een verzoek tot verbeteren, wissen, beperking van de verwerking of een bezwaar tegen de verwerking moeten het aanspreekpunt informatieveiligheid of de data protection officer een nazicht inplannen om, **voor het verstrijken van 6 weken** na deze beslissing, een controle uit te voeren op de databases om na te gaan of deze actie volledig werd uitgevoerd, en hierna indien nodig bijkomende acties in te plannen.

De betrokkene dient geïnformeerd te worden over het resultaat van dit nazicht, en de eventuele acties die daarna worden gepland.

4. Richtlijnen

4.1. Richtlijnen informatieveiligheid

4.1.1. Omgaan met wachtwoorden

Kiezen van wachtwoord

Kies voor alle toepassingen een complex en sterk wachtwoord. Kenmerken van een sterk wachtwoord:

- Gebruik een lang wachtwoord. Een wachtwoord moet minimaal 13 tekens lang zijn.
- Combineer cijfers, hoofdletters, kleine letters en symbolen.
- Sterke wachtwoorden zijn doorgaans niet zo gemakkelijk om te onthouden. Je kan ook een wachtwoordzin gebruiken die alleen voor jou betekenis heeft. Als algemene regel geldt dat wachtwoordzinnen op grond van hun lengte veiliger zijn dan zogenaamd „sterke" (complexe) wachtwoorden. Hoe kan je te werk gaan?:
  - Neem een zin die u kan onthouden.
  - Kies zinnen die enkel voor jou betekenis hebben; niet zomaar een opeenvolging van bestaande woorden
  - Neem van ieder woord de eerste letter.
  - Vervang bepaalde letters door leestekens, cijfers, hoofd- en kleine letters
  - Indien toegestaan kan ook de gehele zin ingevoerd worden
  - Keer woorden om
- Gebruik geen
  - persoonlijke gegevens (geboortedatum,…)
  - woord uit het woordenboek
  - bekende uitdrukking, bv. carpe diem
  - bekende trucs, 112233
  - veel herhaling, vb. aaabbb111
  - teller, zoals 'Carpediem1', ' Carpediem2', ' Carpediem3'...
- Herhaal geen karakters, zoals 'aaabbbccc'

- Gebruik waar mogelijk 2-factor-authenticatie. Dit is een extra stap tijdens het login-proces (authenticatie) en is een veiliger methode om in te loggen, doordat het een tweede of derde authenticatie vereist.

Beschermen van wachtwoorden

Wachtwoorden mogen niet medegedeeld worden aan andere gebruikers. Geef je wachtwoord dus aan niemand door. Ook niet wanneer er naar gevraagd wordt door vertrouwelijke personen.

Een gebruiker mag anderen niet toelaten om met zijn wachtwoord en zijn toegangsrechten te werken. Het is uiteraard verboden zelf gebruik maken van de identificatiegegevens (login) van een andere persoon. Leidinggevenden zullen niet vragen naar het paswoord van de medewerkers en geven hun eigen paswoord niet door aan secretariaatsmedewerkers of andere collega's.
Als iemand je wachtwoord vraagt, verwijs dan naar deze richtlijnen rond wachtwoorden.

Hergebruik geen wachtwoorden. Gebruik voor de diverse applicaties een totaal verschillend wachtwoord.
Vermijd het gebruik van hetzelfde wachtwoord voor werk en privé.
Noem geen wachtwoorden in het publiek, per telefoon, via e-mail of niet-versleutelde communicatie.
Wees voorzichtig als je je wachtwoord ingeeft. Zorg ervoor dat niemand kan meekijken.

Verander regelmatig je wachtwoord (om de 6 maand, of zoals opgelegd door de dienst). Doe dit in elk geval onmiddellijk na de eerste login en als dit door de systeem- of netwerkbeheerder gevraagd wordt (zoals bv. na vaststelling van een inbraak). Wijzigen van het wachtwoord kan je zelf.

Medewerkers met kritische functies, in de zin van grotere toegang tot het interne netwerk, bv. IT-medewerkers, applicatiebeheerders, consultants… veranderen hun wachtwoord frequenter (2-maandelijks).

Wachtwoorden van personen met de rol administrator van IT-systemen, worden in een gesloten omslag op een beveiligde plaats in bewaring gegeven. Dit kan, bij afwezigheid van de gebruiker, gebruikt worden als de dienstverlening in het gedrang dreigt te komen. Enkel de IT-manager kan beslissen deze omslag te openen. Indien dit gebeurt moet de gebruiker zo vlug mogelijk verwittigd worden en moet hij zijn wachtwoord wijzigen.

Belangrijk is ook hoe je met je wachtwoorden omgaat. Het is nutteloos om elke zes maanden je wachtwoorden te veranderen of een lange wachtzin te gebruiken om dan je wachtwoord in een document op je computer op te slaan of op een post-it op je computer te hangen. Wees dus voorzichtig waar je je wachtwoorden bewaart, sla ze nooit zichtbaar op.
Bewaar je wachtwoord niet in een browser, in je mail, in een word-document, op een post-it bij je computer, in notitie op je smartphone.
Je kan voor de opslag van wachtwoorden gebruik maken van een bekende wachtwoordkluis en die beveiligen met een wachtzin.

Als je verneemt dat één van de websites waarop je een account hebt, gehackt wordt, neem je contact op met de Helpdesk. Zodra het probleem bij de website opgelost is, pas je je wachtwoord aan.

Wachtwoorden zijn persoonlijk en vertrouwelijk. Iedere personeelslid is verantwoordelijk voor het gebruik van zijn gebruikersnaam en wachtwoord.

Wees kritisch bij ontvangen van mails of telefoons waarin gevraagd wordt je wachtwoord door te geven of te wijzigen. Reageer hier niet op en meld dit.

Het is verboden wachtwoorden van anderen te kraken.

Bij vermoeden of vaststellen van misbruik of inbreuken, meld je dit zo snel mogelijk weten aan het Meldpunt

4.1.2. Verwijderbare media

Verwijderbare media zijn middelen waarop digitaal opgeslagen gegevens kunnen worden bewaard, die afzonderlijk van een systeem kunnen worden bewaard.
Voorbeelden:

- USB-sticks
- Geheugenkaarten
- Externe harde schijven
- CD’s en DVD’s
- …

Synoniem: externe dragers

Ze worden gebruikt voor transport van informatie. Deze media zijn handig, maar ze vormen ook een beveiligingsrisico zoals gegevensverlies en introduceren van schadelijke software (malware).

Bij verlies van dergelijk medium, kan de inhoud in handen van derden vallen. Dit is een probleem indien persoonsgevoelige en vertrouwelijke gegevens werden opgeslagen. Met persoonsgegevens moeten we conform de wet- en regelgeving omgaan. Dit impliceert dat we er voorzichtig moeten mee omspringen en beveiligen tegen toegang door onbevoegden.

Bovendien

- kunnen onbevoegden die toegang krijgen tot de informatie op verwijderbare media, de informatie:
  - manipuleren (wijzigen, vernietigen)
  - ongeoorloofd verspreiden (in oorspronkelijke of gemanipuleerde vorm)
- kan het aansluiten van dergelijke media ons netwerk infecteren, als de inhoud van zo'n opslagmedium besmet is met een of meerdere virussen.

Omdat we de vertrouwelijkheid, integriteit en beschikbaarheid van persoonsgegevens en vertrouwelijke informatie moeten beschermen tegen inbreuken, wordt dit soort informatie niet opgeslagen op verwijderbare media.

Verwijderbare media, bv. USB-sticks worden intern, niet standaard gebruikt om gegevens uit te wisselen, behalve als er geen alternatieve manier mogelijk is (bv. via internet).

Persoonlijke verwijderbare media zijn niet toegelaten. Enkel de verwijderbare media die door de dienst ter beschikking worden gesteld, mogen worden gebruikt. Systeem-USB-sticks zoals zelfstartende, zijn niet toegelaten. Indien vanuit de organisatie USB-sticks worden meegegeven als geschenk, moet ze voldoen aan deze richtlijnen.

Alle informatie moet geback-upt worden op infrastructuur van GO!, niet via verwijderbare media.

De gebruiker is verantwoordelijk om de USB-stick of de andere gebruikte verwijderbare media te formatteren na gebruik.

Draag zorg voor verwijderbare media, zowel op de werkvloer, onderweg als op een andere locatie. Laat ze niet onbeheerd achter.

4.1.3. Omgaan met e-mail

E-mail wordt gebruikt als een professioneel communicatiemiddel. Mails hebben vaak een informeler karakter. Toch gelden dezelfde regels als bij andere vormen van communicatie. Daarom is het belangrijk dat gebruikers er zich bewust van zijn dat ze e-mail op een correcte en verantwoorde manier moeten gebruiken.

Algemene richtlijnen

- Elke medewerker van het GO! krijgt een mailaccount. Om toegang tot e-mail te bekomen, verstrekt het GO! de gebruiker een e-mailadres, gebruikersnaam en wachtwoord. Gebruik voor het versturen van mails steeds je eigen login en wachtwoord. Ga daarbij op een verantwoorde manier om met je wachtwoord (zie richtlijnen rond wachtwoorden).

- Behandel professionele mails steeds in de aangeboden mailprogramma's van het GO!. Verstuur professionele mails steeds vanuit je GO!-mailadres. Stuur ze niet door naar een eigen, externe mailbox om ze van daaruit te behandelen.

- Communiceer steeds op een correcte manier.

- Wees beleefd, gebruik gepaste taal en schrijf met respect
- Stuur neutrale berichten, dus geen mails met commercieel, politiek of religieus karakter
- Stuur geen mails waarvan de inhoud
  - beledigend is
  - in strijd is met de openbare orde, goede zeden, wet- en regelgeving
  - discriminerend, racistisch of xenofobisch is
  - het privé-leven van iemand kan aantasten
  - iemand schade kan berokkenen
  - de mededeling van gegevens bevat die auteursrechtelijk beschermd zijn of in strijd is met de wetten ter bescherming van dit recht
  - …
- Maak geen gebruik van mail voor geladen boodschappen of discussies. Gevoelige zaken los je beter mondeling op.

- Het gebruik van het e-mailsysteem van het GO! is verboden in geval van betrokkenheid bij illegale, frauduleuze of kwaadwillige activiteiten.
  - Stuur geen mails die onwettige informatie bevatten zoals o.a. hacking software.
  - Verstuur geen kettingbrieven, virusberichten, spam.
  - Vervals geen e-mail (vb. mails versturen vanuit het account van iemand anders,…).

- Ga op een verantwoorde en efficiënte manier om te gaan met mail om overvolle mailboxen te vermijden. Verkies persoonlijk contact of de telefoon boven mail, zeker voor dringende zaken.

- Reageer binnen redelijke tijd na het ontvangen van een mail. Dit is een belangrijk aspect binnen de dienstverlening van het GO!. Enkel als je in 'Aan' geadresseerd staat, wordt verwacht te antwoorden.

- Schrijf gestructureerde mails.

- Geef steeds een duidelijke, korte omschrijving in de onderwerpsregel (a.d.h.v. sleutelwoorden)

- Wees zuinig met CC, BCC, allen beantwoorden. Zet enkel de persoon van wie je actie verwacht in Aan en vermeld duidelijk wat je verwacht. Stuur het bericht enkel naar die personen die echt op de hoogte moeten zijn of expliciet om een kopie gevraagd hebben. Voeg uw leidinggevende dus niet systematisch in alle mails in CC toe. Gebruik BCC indien geadresseerden elkaars contactgegevens niet mogen kennen.

- Stem met andere diensten en collega's af vooraleer een antwoord naar externen te mailen. Vaak veronderstelt een antwoord aan externen voorafgaand overleg of discussie. Een antwoord naar externen is steeds het gemeenschappelijk, afgestemd antwoord van de dienst.
  Interne voorbereidingen of discussies worden niet opgenomen in de mail naar externen.

- Beperk bijlagen qua aantal en grootte. Definieer steeds duidelijk hun inhoud.

  Verwijs indien mogelijk via een link naar de locatie waar het document zich bevindt. Doe dit zeker bij intern mailverkeer. Indien je een bericht met één of meerdere bijlagen ontvangt en dit bericht dient te beantwoorden of door te sturen, ga dan op voorhand na of het nodig is de bijlage(n) toe te voegen, zodat de grootte van de berichten die worden doorgestuurd en opgeslagen, beperkt kan worden.

  Audio- en videobestanden worden niet doorgestuurd in bijlage. Deze bestanden kunnen immers risico's inhouden en de systemen wijzigen of virussen kan bevatten. Voor het raadplegen van dit type bestanden wordt een link verstuurd naar de locatie waar het bestand zicht bevindt. Bij communicatie naar externen kan deze locatie bv. YouTube of een ander kanaal zijn.

- Alleen voor heel dringende berichten gebruik je prioriteit hoog.
- Elk personeelslid stelt een professionele, digitale handtekening in zoals opgelegd door het GO! zodat jouw naam en contactgegevens vermeld staan. Gebruik alleen de eigen handtekening.
- Er werd door het GO!/de dienst een disclaimer toegevoegd. Breng hier geen wijzigingen aan.
- Het gebruik van een ontvangst-/leesbevestiging kan handig zijn bij belangrijke e-mails waarvan de schrijver wenst te weten of de ontvanger ze ontvangen en/of gelezen heeft.
- Denk na vooraleer je je abonneert op nieuwsbrieven. Het aantal ontvangen mails kan exponentieel de hoogte ingaan als je je hierop inschrijft.
- De ICT dienst beveiligt het emailverkeer op verschillende manieren, tegen virussen, spam.

Professioneel versus persoonlijk gebruik

Het gebruik van de elektronische communicatiemiddelen die ter beschikking worden gesteld door het GO! is bedoeld voor professionele doeleinden.

Elektronische communicatie voor privédoeleinden blijft beperkt en occasioneel, doet geen afbreuk aan de goede werking en veiligheid van het netwerk en de productiviteit van de medewerker of collega's en vormt geen inbreuk op de van kracht zijnde richtlijnen en wet- en regelgeving. Anderzijds wordt een privé e-mailadres ook niet gebruikt voor professionele doeleinden.

Indien je persoonlijke mails ontvangt op je professioneel e-mailadres, worden deze na lezen onmiddellijk verwijderd of in een map 'Privé' of 'Persoonlijk' geklasseerd. Dit geldt ook voor verzonden, privémails. Deze goede praktijk kadert in de bescherming van de persoonlijke levenssfeer van het personeelslid bij toegang tot de mailbox i.k.v. het verzekeren van de continuïteit van de werking of controle.
Vergeet in dit kader ook niet je gespreksgeschiedenis te beheren (verwijderen van berichten die je via Lync verstuurt).

Afwezigheidsassistent

Maak bij afwezigheid gebruik van afwezigheidsboodschappen, zowel voor intern als extern mailverkeer. Je vermeldt hierin wie gecontacteerd kan worden tijdens jouw afwezigheid en wanneer je terug bereikbaar bent. Maak binnen de instelling afspraken betreffende het opvolgen van professionele mails bij afwezigheid van personeelsleden.

Bescherming van vertrouwelijkheid van gegevens

Check de bestemmeling vooraleer u mails verstuurt. Zorg ervoor dat mails niet bij de verkeerde personen terecht komen, zeker indien ze vertrouwelijke gegevens bevatten. Gebruik BCC waar nodig.

Vertrouwelijke gegevens worden niet zomaar via e-mail meegedeeld. Bespreek met uw afdelingshoofd welke informatie verspreid mag worden. Gegevens zoals paswoorden, toegangscodes, gevoelige persoonsgegevens enz. mogen niet via e-mail worden meegedeeld, tenzij op een beveiligde manier.

Veilig omgaan met e-mail

Een aantal kritische rollen zijn verplicht een digitale handtekening in te stellen. Hiermee wordt aangeduid dat een mail echt van deze afzenders komt.

Wees alert bij de behandeling van mails. E-mail is geen waterdicht, veilig communicatiemiddel. Het GO! implementeert technische veiligheidsmaatregelen om te vermijden dat schadelijke toepassingen in de mailbox terechtkomen. Het is verboden deze instellingen te deactiveren of de beveiligingssystemen te omzeilen.

Het openen van bijlagen die afkomstig zijn van onbekende, onbetrouwbare personen kan ernstige gevolgen hebben voor het interne netwerk en voor de gegevens die in dit netwerk zijn opgeslagen. Hetzelfde geldt voor het aanklikken van links die zich in een mail bevinden. Klik niet zomaar een link in een mail aan en wees alert bij het openen van bijlagen. Ga vooraf na wie de verzender is. Zet je leesvenster uit om te voorkomen dat je automatisch virussen binnenhaalt.

Geef je e-mailadres niet aan iedereen en tik het niet zomaar ergens in. Het ingeven van je emailadres op een website of reageren op een mail/forum kan ertoe lijden dat je slachtoffer wordt van spam-mails.

Beheer van mails

Mails worden bewaard bij de dossiers/ op de plaats waar ze horen. Bewaar ze niet in de persoonlijke mailbox maar zorg dat de informatie gedeeld wordt. Klasseer mails zo snel mogelijk, bij voorkeur onmiddellijk bij ontvangen/verzenden en verwijder ze daarna uit de mailbox. Ken een duidelijke, betekenisvolle bestandsnaam toe aan de mail en bijlagen die je opslaat. Zie Werkinstructie Beheer e-mail.

Mailboxen worden regelmatig opgeruimd waarbij relevante mails opgeslagen worden op de plaats waar ze thuis horen en mails met puur informatieve waarde verwijderd worden uit de mailbox.

Vóór uitdiensttreding, veranderen van functie of langdurig verlof wordt de mailbox steeds door het personeelslid opgeruimd.

4.1.4. Omgaan met internet

Inleiding

Het internet wordt in principe gebruikt als een professioneel werkinstrument. Gebruik kan echter een aantal risico's inhouden. Zo kan het bezoeken van bepaalde websites of het downloaden van software schade veroorzaken aan het netwerk. Vandaar de noodzaak aan een beleid voor internetgebruik.

Iedereen is verantwoordelijk voor een correct en verantwoord gebruik en dienen dus als een "goede huisvader" met internet om te gaan.

Algemene gebruiksregels

Het internet wordt gebruikt als professioneel werkinstrument.

Medewerkers houden de configuratie van de webbrowser en de beveiligingssoftware (antivirus, antispam, firewall) zoals ingesteld door de organisatie ongewijzigd.

Medewerkers moeten zich steeds bewust zijn dat ze het GO! vertegenwoordigen op internet. Veel websites houden een spoor bij van bezoek en kunnen soms de herkomst en de elektronische identiteit vaststellen van de persoon en van de organisatie.

Het is verboden de toegang die het GO! tot het internet biedt te gebruiken (niet exhaustieve opsomming):

- voor het raadplegen van websites die
  - aanzetten tot betrokkenheid bij illegale, frauduleuze of kwaadwillige activiteiten;
  - aanzetten tot laster en eerroof;

- informatie met een aanstootgevend, obsceen, pornografisch, discriminerend, racistisch of onterend karakter bevatten, tenzij dit noodzakelijk is binnen uw professionele opdracht, afgestemd met uw leidinggevende;
- informatie met een beledigend, kwetsend en/of bedreigend karakter bevatten;
- aanzetten tot het overtreden van de wet;
- aanzetten tot pesten op grond van geslacht, ras, nationaliteit, fysiek vermogen en andere kenmerken
- …

Het is ook niet toegestaan dergelijk materiaal of andere bedreigende, intimiderende of misleidende berichten of afbeeldingen te downloaden of te verspreiden, tenzij dit noodzakelijk is binnen uw professionele opdracht, afgestemd met uw leidinggevende.

Medewerkers verlaten niet-professionele sites bij vermoeden dat de bezochte site niet is waar naar gezocht werd.

Het is verboden om internet te gebruiken voor illegale activiteiten, ongeacht de aard ervan (fraude, hacking, illegaal bestanden te downloaden, kopiëren en op te slaan, inclusief dergelijke info te verspreiden, bv. van auteursrechtelijk beschermde software, video's, muziek, foto's of documenten... , overtreden wet- en regelgeving,…)

Bij het downloaden van bestanden beperkt de medewerker zich tot het strikt noodzakelijke in het kader van zijn beroepsactiviteiten.

Het internet wordt niet gebruikt voor commerciële of excessieve persoonlijke of recreatieve doeleinden.

Het GO! behoudt zich het recht voor om de toegang tot internet (websites en diensten) te beperken.

Enkel het mailsysteem van het GO! wordt gebruikt voor de behandeling van professionele mails. Er worden, voor professionele doeleinden, geen andere e-mailsystemen via het internet gebruikt. Zie richtlijnen rond gebruik van e-mail.

Professioneel en privé-gebruik

Net zoals alle andere werkmiddelen die ter beschikking worden gesteld, is het de bedoeling dat internet als een professioneel instrument gebruikt wordt. Beperkt privé gebruik is toegestaan onder bepaalde voorwaarden. Het mag :

- de uitvoering van de taken en de productiviteit niet belemmeren;
- collega's niet storen bij de uitvoering van hun taken;
- geen inbreuk vormen op de policies en procedures.

Het onevenredig en onredelijk gebruik is niet toegelaten. Het buitensporig downloaden, reproduceren, creëren, verspreiden en bewaren van gegevens die niet in verband staan met de professionele activiteiten van het GO!, worden als storende activiteiten beschouwd. Het buitensporig karakter heeft betrekking op het gebruik van arbeidstijd, transportcapaciteit, verwerkingscapaciteit en/of opslagruimte. Zo is het onder

Veilig omgaan met internet

Internet is een krachtig instrument waarmee we heel wat informatie kunnen terugvinden en uitwisselen. Het gebruik van internet houdt echter ook een aantal risico's in. Cybercriminelen verspreiden virussen en malware met als mogelijk gevolg diefstal, onrechtmatige inzage, wijziging, verspreiding en vernietiging van (vertrouwelijke) gegevens.

Enerzijds vangt technische beveiliging deze risico's voor een groot deel op. De IT-dienst van het GO! implementeert verschillende veiligheidsvoorzieningen om zich te wapenen tegen aanvallen, zowel intern als extern. Elke poging tot aanval, deactivering, wijziging van de configuratie, omzeiling van de beveiligingssystemen is dan ook verboden.

Anderzijds is ook het gedrag van de gebruiker van groot belang om de risico's te beperken.
Wees alert voor twijfelachtige URL's, download-voorstellen en ga niet in op pop-upvensters of ongevraagde reclameberichten.
Verlaat meteen de website indien u vermoedt of vaststelt dat de site niet van de organisatie is die u voor ogen had.
Controleer welke URL er achter een link schuil gaat door met de muis over een link te gaan zonder die aan te klikken. De echte link wordt zichtbaar die je vervolgens kan analyseren.
Indien vertrouwelijke gegevens op elektronische wijze worden overgemaakt, dienen de gepaste maatregelen te worden getroffen om de vertrouwelijkheid en de integriteit van de overgemaakte gegevens te waarborgen, met inachtneming van de van kracht zijnde wetgevingen en reglementen.
Een beveiligde verbinding herken je aan https:// aan het begin van de URL.
Controleer steeds op https:// aan het begin van het webadres voor u persoonlijke/gevoelige informatie invoert.
Als een website vraagt om persoonlijke gegevens in te voeren, stel je dan de vraag of dit wel noodzakelijk is deze informatie te verschaffen. Geef ook niet zomaar overal je emailadres op zodat dit niet in handen komt van spammers.
Gebruik de unsubscribe-optie in een spambericht niet (je bevestigt hiermee je e-mailadres richting de spammer). Open geen non Delivery Report-berichten van berichten die je niet verstuurd hebt.
Indien een pop-up u gevaarlijk lijkt, sluit deze niet af met het kruisje. Ga via Ctrl+ALT+DEL naar Taakbeheer en sluit uw internetbrowser af.

Werk steeds op de aangeboden beveiligde omgeving van het GO!. Indien je via wifi op internet gaat, gebruik dan het draadloos netwerk aangeboden door de instelling van GO!. Het gebruik van veilige/vertrouwde netwerken is ook een must voor gebruik van wifi als u op een andere locatie werkt.

Medewerkers kunnen zelf geen software installeren. Er moet nl. op voorhand worden nagegaan of een softwareprogramma afkomstig is van een betrouwbare bron, of er geen tegenstrijdigheid bestaat met het licentiebeleid en of er een risico bestaat op het vlak van informatieveiligheid of privacy vooraleer dergelijk softwareprogramma te installeren.

4.1.5. Clean desk – clear screen

Inleiding

Een deel van de informatie die door het GO! wordt verwerkt, is vertrouwelijk en moet beschermd worden tegen ongeoorloofde toegang.

Bij de bescherming van informatie tegen ongeoorloofde toegang, speelt de gebruiker een cruciale rol. Zowel in de omgang met papieren documenten als bij de toegang tot digitale systemen is de hulp van de medewerkers van essentieel belang voor een goede informatiebeveiliging.

In dit kader wordt van de medewerkers gevraagd onderstaande goede praktijken na te leven. Deze praktijken dienen steeds om te waarborgen dat de toegang tot informatie beperkt is tot de personen die er recht op hebben en dat het risico van ongeoorloofde toegang tot informatie, -verwerkende systemen en materialen of beschadiging ervan tot een minimum beperkt wordt.

Algemeen

Gevoelige informatie of dragers ervan mogen nooit onbewaakt achtergelaten worden. Dit geldt niet alleen op de werkplek maar ook onderweg, op externe locaties en in alle ruimtes waar zich informatie, informatie-verwerkende systemen, IT-systemen of materialen bevinden, bv. datalokaal, vergader- en leslokalen, stock ICT, het archief. Dit houdt in dat deze informatie en dragers (laptops, USB-sticks, smartphones,…) op zodanige wijze opgeborgen worden dat deze enkel toegankelijk zijn voor bevoegde medewerkers. Bij twijfel worden ze steeds veilig opgeborgen.
Met gevoelige gegevens bedoelen we zowel persoonsgevoelige als vertrouwelijke (bv. organisatie-kritische) informatie.

Vernietigen van informatie en dragers verloopt steeds volgens de voorziene procedures (zie Procedure Vernietigen Documenten en Procedure Vernietigen ICT-middelen). Archiefruimtes zijn steeds op slot en er zijn afspraken vastgelegd over de toegang en raadpleging/ontlening.

Er gelden drie basisregels:

1. Wanneer de medewerker op kantoor aanwezig is : de medewerker probeert enkel de documenten die hij die dag nodig heeft op zijn bureau te laten liggen.

2. Wanneer de medewerker tijdelijk zijn bureau verlaat: indien de medewerker bv. vaak aan vergaderingen deelneemt, moet hij/zij controleren of er geen vertrouwelijke informatie aanwezig is op zijn bureau die onbewaakt mag worden achtergelaten. Indien dit wel het geval is, moet hij/zij deze informatie veilig opbergen. Bovendien moet hij/zij bij een langere afwezigheid minimaal de computer in slaaptoestand zetten en beveiligen aan de hand van een paswoord.

3. Wanneer de medewerker zijn bureau verlaat: het is de taak van de medewerker om ervoor te zorgen dat alle gevoelige informatie op een veilige plaats wordt opgeborgen zoals een kast die op slot kan en dat zijn bureau is opgeruimd alvorens de organisatie te verlaten. Kasten met gevoelige informatie worden steeds op slot gedaan (dit kan ook de afspraak zijn voor de lokalen/bureaus).

Concreet

Bij afsluiten van de werkdag:

- meld af en sluit de computer/laptop af;
- berg je dossiers of documenten, materiaal (muis, klavier en muismatje), mobiele toestellen, persoonlijke bezittingen of andere zaken op in de kast en persoonlijke locker.
- Sluit kasten met gevoelige informatie/toestellen

Indien je de werkplek voor langere tijd verlaat (bv. om naar een overleg in huis te gaan):

- Vergrendel je de computer. Omdat vergeten menselijk is, wordt de computer na 15 minuten automatisch vergrendeld.
  Ook mobiele toestellen hebben steeds een beveiligingscode en zijn vergrendeld indien ze niet gebruikt worden.
- Berg je gevoelige documenten en dossiers op in gesloten kast. Zo kan informatie niet (per ongeluk) in de verkeerde handen terecht komen.
- Laat ook je badge, sleutels en mobiele toestellen niet onbeheerd achter (bv. bij verlaten van je bureau om naar een overleg te gaan, tijdens je verplaatsing naar een externe locatie).

Documenten en dossiers op papier die gevoelige gegevens bevatten, worden in gesloten kast bewaard. Maak afspraken met collega's over de toegang en het bewaren van de sleutels.

Gevoelige informatie wordt niet genoteerd op post-its of andere materialen die dienst doen als geheugensteuntje. Verwijder flipcharts of andere materialen met gevoelige informatie na afsluiten van een vergadering, vorming/nascholing/studiedag.

Laat geen papieren achter bij de printer. Controleer of wat je afprint volledig is. Bezorg achtergebleven prints steeds aan de betrokken persoon indien u dit opmerkt. Geef ze niet door aan onbevoegden. Draag ook zorg voor de papieren documenten die je mee neemt op verplaatsing (vergaderingen al dan niet buitenshuis,…).
Werk steeds binnen de digitale omgeving zoals voorzien en opgelegd door het GO!. Computers en mobiele toestellen zijn steeds voorzien van een sterk wachtwoord (zie richtlijnen over wachtwoorden).

Er wordt ook voorzichtig omgesprongen met verwijderbare media (USB-sticks,…). Deze worden niet onbeheerd achtergelaten.

Laat geen informatie achter op een smartboard.
Plaats geen gevoelige documenten op het bureaublad.

4.1.6. Omgaan met sociale media:

Onder sociale media verstaan we interactieve internettoepassingen die een multimediale dialoog tussen gebruikers van het medium mogelijk maken. Cruciaal daarbij is dat de gebruiker niet alleen consumeert maar ook gemakkelijk zelf inhoud aan het medium toevoegt. Het is tweerichtingsverkeer http://communicatie.vlaanderen.be/nlapps/docs/default.asp?fid=171

Deze procedure handelt over alle vormen van sociale media, o.a.:
- Sociale netwerken (Facebook, Twitter, LinkedIn, WhatsApp, …)
- Audio- en videotoepassingen (Youtube, Instagram, Flickr, Snapchat,…)
- Collectieve encyclopedieën (Wikipedia)
- Blogs
- Publieke discussiefora
- Andere en toekomstige, gelijkaardige tools

Wie? De gebruiker

Het GO! is actief op sociale media. Deze media bieden heel wat kansen. Ze stellen het GO! in staat om met een breed publiek in dialoog te gaan. Op die manier kan informatie gedeeld worden, kunnen de relaties met gebruikers versterkt worden en kan de bekendheid van het GO! uitbreiden. Het gebruik van sociale media kan dus een grote impact voor het imago hebben. Anderzijds kunnen verkeerd gebruik en misbruik ervan echter schade berokkenen aan het GO! of derden. Het GO! verwacht daarom van de personeelsleden dat ze op een verantwoorde manier met deze media omgaan.

Ook derden gebruiken deze media. Het GO! wil enerzijds positieve boodschappen over haar werking gebruiken en waarderen. Anderzijds wil ze ook op de hoogte zijn van negatieve commentaren om dit te gebruiken in kader van haar dienstverlening en zelfevaluatie. Hierbij rekent het GO! op de melding door haar personeelsleden.

Ook heel wat werknemers zijn voor privé-gebruik actief op sociale media.

Richtlijnen

Onderstaande richtlijnen helpen de gebruiker in de omgang met sociale media. Bij het gebruik ervan gelden ook de richtlijnen rond gebruik van internet en e-mailgebruik.

Professionele communicatie gebeurt altijd via de sociale media-accounts van het GO!. Deze accounts zijn dan ook uitsluitend bedoeld voor professionele doeleinden. Het is niet toegelaten ze te gebruiken voor persoonlijke doeleinden.

Wees je ervan bewust dat sociale media grotendeels publiek zijn en wat je schrijft voor onbepaalde tijd openbaar en zichtbaar kan zijn.

Wees duidelijk over je (professionele) identiteit. Professioneel gezien, handel je in naam van het GO!.

Je bent verantwoordelijk voor wat je schrijft over het GO! of haar partners op blogs, fora en andere sociale media.

- Schrijf steeds respectvol.
- Neem een positieve houding aan.
- Wees relevant en schrijf korte, duidelijke berichten.

Sociale media mogen niet worden gebruikt voor

- aanzetten tot of betrokkenheid bij illegale, frauduleuze of kwaadwillige activiteiten;
- laster en eerroof;
- verspreiden of delen van informatie (berichten, foto's, filmpjes,…) met een aanstootgevend, obsceen, pornografisch, discriminerend, racistisch of onterend, beledigend, kwetsend en/of bedreigend karakter;
- het overtreden van de wet of aanzetten hiertoe;
- pesten (aanzetten tot en betrokkenheid bij pesten)
- het plaatsen van spam
- het verspreiden van niet-correcte informatie
- … (lijst niet-exhaustief)

Respecteer de wet- en regelgeving, o.a. het auteursrecht, het recht op afbeelding,... Publiceer geen foto's van anderen zonder hun uitdrukkelijke toestemming.

Respecteer de persoonlijke levenssfeer van anderen.

Verspreid geen vertrouwelijke informatie op sociale media.

Gebruik sociale media niet voor geladen discussies of boodschappen. Vermijd persoonlijke aanvallen en gevechten. Schrijf geen ongepaste/negatieve commentaren over collega's, de leidinggevende of de organisatie. Publiceer niets waar je spijt van krijgt.

Schrijf enkel over onderwerpen die tot je eigen expertise behoren. Berichten die hierbuiten vallen, laat je over aan de betrokken collega/expert.

Let op je privacy-instellingen per Sociale Media-account. Hiermee kun je over het algemeen nauwkeurig instellen wie jouw berichten wel of niet mogen zien. http://www.mijnonlineidentiteit.nl/social-media-privacy-instellingen/

Professioneel versus privé-gebruik

GO!-medewerkers kunnen tijdens de diensturen actief zijn op sociale media mits het werkgerelateerde content betreft en het ander werk hier niet onder lijdt.

Gebruik van sociale media voor privédoeleinden is toegestaan op voorwaarde dat dit slechts occasioneel gebeurt en redelijk blijft, geen afbreuk doet aan de goede werking en veiligheid van het netwerk en de productiviteit van de medewerker of collega's en geen inbreuk vormt op de van kracht zijnde wet- en regelgeving.
Voor privé-doeleinden kunnen enkel de persoonlijke socialemedia-accounts gebruikt worden. In je privé-gebruik blijf je loyaal aan het GO! en verspreid je geen werkgerelateerde informatie.

Ook buiten de arbeidstijd wordt van het personeelslid loyauteit t.a.v. het GO! als werkgever verwacht. Via privé-accounts wordt geen professionele informatie verspreid. Het is niet toegestaan om vertrouwelijke informatie van het GO! of betrokken personen of diensten/organisaties bekend te maken of handelingen te stellen die schade aan de werkgever of derden kunnen berokkenen. Het is niet toegestaan persoonlijke denkbeelden te doen overkomen als die van de organisatie.

Het is GO!-personeelsleden toegestaan om in privé-situaties werkgerelateerde onderwerpen te publiceren mits het geen vertrouwelijke informatie over het GO! en haar partners betreft en deze geen schade kan berokkenen. Indien deelgenomen wordt aan gesprekken over het GO!, moet de persoon steeds vermelden dat hij een GO!-medewerker is.

4.1.7. Vernietiging van documenten

Bij vernietiging van informatie moeten we er steeds alert voor zijn dat informatie die niet openbaar mag worden, beschermd wordt tegen inzage door onbevoegden.

De vernietiging van overheidsinformatie is wettelijk geregeld. Voor de vernietiging van archiefdocumenten is het Archiefdecreet van 9 juli 2010 van toepassing. In art. 12 wordt bepaald dat een zorgdrager enkel op basis van een goedgekeurde selectielijst kan overgaan tot vernietiging van archiefdocumenten. Een selectielijst wordt gelijk gesteld met een informatiebeheersplan.

Om documenten correct te kunnen vernietigen, moeten we momenteel een procedure ad-hoc vernietiging doorlopen. Een ad-hoc vernietigingsaanvraag is een vernietiging die gebeurt zonder dat hiervoor richtlijnen zijn opgenomen in een vastgestelde selectielijst.

In een eerste stap wordt een verklaring voor vernietiging ingevuld (sjabloon). Hierin wordt opgelijst welke documenten in aanmerking komen voor vernietiging en waarom ze vernietigd mogen worden. Deze afweging wordt gemaakt op basis van de administratief-juridische bewaartermijn en de vraag of de documenten permanente cultureel-maatschappelijke waarde hebben.

De vraag om toestemming tot vernietiging wordt voorgelegd aan de leidinggevende van de instelling/dienst. Na toestemming van de leidinggevende wordt de lijst bezorgd aan sofie.descamps@g-o.be die de vraag tot toestemming indient bij de Selectiecommissie Vlaamse overheid.
Deze voert een inhoudelijke en vormelijke kwaliteitscontrole uit en kent de goedkeuring al dan niet toe.

Van zodra de verantwoordelijke voor het archiefbeheer de toestemming ontvangen heeft, wordt dit teruggekoppeld naar de dienst die kan overgaan tot de effectieve vernietiging.

Vernietigingen gebeurt op basis van de classificatie van informatie:

- Persoonsgevoelige, strategische of andere gevoelige informatie die niet bestemd is voor derden wordt vernietigd door een gespecialiseerde firma die een attest levert.
- Documenten zonder persoonsgevoelige, strategische of andere gevoelige informatie kan worden meegegeven met de papierophaling.

Na de vernietiging wordt de gedateerde verklaring van vernietiging vervolledigd met de datum en plaats van de effectieve vernietiging en wordt deze bewaard.

Bij schonen van archief dient geen toestemming te worden gevraagd. Bij schonen van bijvoorbeeld dossiers bewaart u de dossiers zelf, maar verwijdert u alle dubbels, blanco's, kladjes, documentatie…

Voorbeelden van stukken die verwijderd kunnen worden zijn:

- dubbels, kopieën, blanco's en lege formulieren

- werkdocumenten met een louter tijdelijk belang, bv. circulaires, excels met tijdelijke taakverdelingen, ontvangstmeldingen, uitnodigingen voor vergaderingen ... tenzij die van administratief-juridisch belang zijn
- drukwerk dat louter ter informatie werd toegevoegd (folders, brochures, documentatie, nieuwsbrieven …)
- grote metalen hechtingsmechanismen (nietjes, paperclips ...)
- ringmappen en ordners (klasseurs), dus niet de inhoud, maar wel de map zelf
- plastiek en elastiek
- voorgaande en kladversies van een document, tenzij deze van belang zijn om de ontstaansgeschiedenis van een bepaald document of beslissing te reconstrueren. Bij wet- en regelgeving kan het bijvoorbeeld wel van belang zijn om voorgaande versies te bewaren.

Het schonen van archief zorgt ervoor dat dossiers op lange termijn beheersbaar zijn en dat enkel de noodzakelijke stukken bewaard blijven.

Ook hier wordt rekening gehouden met de aard van de documenten en wordt het onderscheid gemaakt tussen documenten die mee kunnen met de papierophaling en documenten die versnipperd/vernietigd worden door een gespecialiseerde firma.

De certificaten van vernietiging worden bewaard door de dienst.

Het is ook belangrijk op te merken dat er geen vernietigingsplicht bestaat. Elke zorgdrager heeft dus het recht om documenten die in de selectielijst als 'te vernietigen' staan aangemerkt, toch permanent te bewaren

ICT-middelen

Ook bij de vernietiging ICT-middelen moeten we er steeds alert voor zijn dat de informatie die aanwezig is op deze middelen en niet openbaar mag worden, beschermd wordt tegen inzage door onbevoegden.

ICT-middelen worden uit dienst genomen als ze technologisch achterhaald zijn of wegens defect niet correct meer functioneren. De overhandigde IT-middelen worden gestockeerd in een beveiligde opslagplaats. Alleen geautoriseerde personen hebben toegang tot deze opslagplaats.

Een erkende firma vernietigt het materiaal op gepaste wijze en levert hiervan attesten. Deze attesten van vernietiging worden bewaard.

4.1.8. Documentbeheer

Algemeen

Bij de uitvoering van de dagelijkse taken worden heel wat documenten opgemaakt of ontvangen. Deze documenten ondersteunen de dagelijkse bedrijfsvoering en dienstverlening en de interne processen.

Om efficiënt en klantgericht te kunnen werken, is het van belang een goede en betrouwbare informatiehuishouding uit te bouwen. Een van de pijlers hierbij is een degelijk documentbeheer.

De uitgangspunten van een goed documentbeheer zijn:
- centrale opslag van documenten. Professionele documenten horen thuis binnen de informatiesystemen van het GO!. Hierbij kan het gaan om applicaties, de G-schijf en cloud-oplossingen;
- delen van documenten zodat collega's over de informatie kunnen beschikken die ze nodig hebben en waartoe ze vanuit hun rol en taak bevoegd zijn;
- dossiervorming: alle documenttypes binnen een dossier worden samen opgeslagen, ook e-mails, presentaties, foto's, rekenbladen, nota's,... Op die manier worden volledige en unieke dossiers

gecreëerd die alle informatie bevatten die nodig is om de zaak te behandelen. Dossiervorming is een voorwaarde voor informatiedeling en snel terugvinden van informatie;
- standaardisatie en afspraken rond bestandsnamen;
- toepassen van versiebeheer zodat steeds duidelijk is welke de meeste recente en correcte versie van een document is.

Informatiestromen krijgen steeds een informatie-eigenaar die verantwoordelijk is voor het beheer gedurende de volledige levenscyclus. Deze persoon is best geplaatst om, rekening houdend met de rollen (taken) en wet- en regelgeving, te bepalen wie toegang tot deze informatie mag hebben. Hij staat dan ook in voor de bepaling van de classificatie en gebruiksregels.

Bewaren van bestanden

Vanuit het oogpunt van centrale bewaring van documenten wordt voor elke informatiestroom vastgelegd waar de documenten bewaard moeten worden (G-schijf, applicaties,…).

Bij gebruik van een mappenstructuur worden de afspraken betreffende de opbouw van de structuur gerespecteerd (hoofd- en submappen). Voor elke informatiestroom bepaalt de eigenaar wie de mappen beheert en welk type documenten waar bewaard worden. Deze afspraken worden geformaliseerd.

Bij gebruik van andere informatiesystemen worden eveneens afspraken gemaakt betreffende opslag, benaming en beheer.

Toegang tot informatie wordt bepaald op basis van rollen (Toegangsbeleid).

De algemene richtlijnen en afspraken betreffende het toekennen van map- en bestandsnamen worden toegepast (zie Werkinstructie Bestandsnamen). Hierover worden binnen de afdeling/het team afspraken gemaakt, vastgelegd en gecommuniceerd.

Persoonlijke documenten horen niet thuis in de informatiesystemen van het GO!. Een medewerker kan beschikken over een persoonlijke schijf waar een beperkte hoeveelheid persoonlijke documenten kan worden bewaard. **Maak hiervoor, binnen uw persoonlijke schijf, een map 'persoonlijk' aan.** Het GO! is niet verantwoordelijk voor eventueel verlies van deze documenten. Omgekeerd horen professionele documenten niet thuis op de persoonlijke schijf

Opruimen op trashdagen

Op regelmatige tijdstippen worden trashdagen georganiseerd. Op deze dagen wordt:
- nagegaan welke documenten
  - geschoond kunnen worden
  - in aanmerking komen voor vernietiging, dit a.d.h.v. het informatiebeheersplan van de dienst
  - overgedragen kunnen worden aan het archiefdepot van het Huis van het GO! en het archiefdepot van de Vlaamse overheid te Vilvoorde
  - overgedragen kunnen worden naar een digitale archiefmap
- de mailbox opgeruimd. Dit houdt in dat nagegaan wordt:
  - welke mails verwijderd kunnen worden
  - welke mails in de informatiesystemen moeten worden opgeslagen
- de mappenstructuur/informatiesystemen opgeruimd, geëvalueerd en bijgestuurd

4.2. Richtlijnen gebruik van sociale media

Nog aan te vullen

4.3. Richtlijnen foto's en video

4.3.1. Uitgangspunten

Het **recht op afbeelding is een persoonlijkheidsrecht, ook wel portretrecht genoemd. Dit** is een recht waarbij voor het maken van elke menselijke afbeelding, maar ook voor het gebruik (bv. publiceren, verspreiding, …) van die afbeelding uitdrukkelijke toestemming d.m.v. een verklaring of een ondubbelzinnige actieve handeling vereist is van de afgebeelde persoon. Het recht is van toepassing op alle beeldmateriaal waarop mensen herkenbaar of identificeerbaar in beeld komen. Het recht op gebruik van beeldmateriaal staat volledig los van het auteursrecht van de fotograaf. **Herkenbaar**: dat het gezicht niet zichtbaar is, houdt niet automatisch in dat een persoon onherkenbaar wordt afgebeeld. Zo kan een persoon wiens gezicht onherkenbaar is op een foto, toch te identificeren zijn doordat hij bijvoorbeeld een zeer herkenbare trui draagt. Bron: Ik beslis (Privacycommissie), Het recht op afbeelding. Als personen te identificeren zijn in bepaalde situaties, is toestemming nodig voor het gebruik van foto's. Lespakket voor de tweede en derde graad secundair onderwijs. Versie 2.0 augustus 2017

Noot: Bovenstaande betreft een korte, niet-limitatieve duiding over het recht op afbeelding.

Onderscheid

- Gerichte beelden:
  - Toestemming vragen voor het nemen van de foto/maken van het filmpje
  - Toestemming vragen voor het publiceren op een bepaald kanaal. Voor elk kanaal/elke verspreidingsvorm is toestemming nodig.
- Niet-gerichte beelden: sfeerbeelden/spontane beelden
  - Het volstaat dat je de betrokken personen inlicht over het feit dat dergelijke beelden zullen worden genomen, voor welk doel je dat doet en om welke publicatie het gaat.
    Opgelet: Als personen duidelijk weigeren om op de foto te staan, mag je de foto niet nemen.

Toestemming

De toestemming gebeurt door middel van een verklaring of een ondubbelzinnige actieve handeling.
Bij toestemming geldt steeds het recht om te allen tijde zijn gegeven toestemming weer in te trekken. Het intrekken van de toestemming is even eenvoudig als het geven ervan.

Opmerking: Ook de Privacycommissie geeft aan dat je niet van tevoren alle scenario's kan opmaken om alles af te dekken. Het zullen steeds de concrete omstandigheden/de context zijn die nagekeken moeten worden om te bepalen wat je moet doen.

4.3.2. Leerlingen

De Privacycommissie geeft aan dat de schriftelijke toestemming best wordt verkregen via een specifiek toestemmingsformulier. Op dit formulier moet de school nauwkeurig de soorten foto's en filmpjes aanduiden die genomen worden, zoals bijvoorbeeld klasfoto's. De verspreidingsvorm moet ook genoteerd worden zodat duidelijk is of de klasfoto alleen een papieren versie zal kennen of ook op de schoolwebsite en/of op de Facebookpagina van de school terecht komt.

Het is immers zo dat in een besloten kring een onderscheid wordt gemaakt al naargelang de beelden gericht of niet-gericht zijn. Wat nu precies "gericht" en "niet-gericht" is, hangt sterk af van de context en wordt geval per geval bekeken.

Een "**gericht**" beeld slaat veeleer op

- een beeld van een individu of
- een beeld waarin één of enkele personen tijdens een groepsactiviteit worden uitgelicht
- of wanneer voor een afbeelding geposeerd wordt. Een goed voorbeeld hiervan zijn de klassieke klasfoto's of een individuele foto

Bij een "**niet-gericht**" beeld gaat het eerder om beeldmateriaal dat een algemene, spontane en niet geposeerde sfeeropname weergeeft zonder daaruit één of enkele personen eruit te lichten. Een groepsfoto van de klas tijdens een boswandeling of sportactiviteit is hier een voorbeeld van. Voor zulke beelden volstaat het dat je de betrokken personen/leerlingen inlicht over het feit dat dergelijke beelden zullen worden genomen, voor welk doel je dat doet en om welke publicatie het gaat. (Ik beslis)

Aangezien de Algemene Verordening Gegevensbescherming (AVG) vereist dat de toestemming onder meer specifiek dient te zijn, moet het mogelijk zijn voor de betrokken kinderen en/of ouders dat zij toestemming geven voor de ene verspreidingsvorm en eventueel niet akkoord gaan voor een andere.

In het schoolreglement is info opgenomen onder Afspraken. Privacywetgeving en beeldmateriaal. In bijlage wordt het model van toestemmingsformulier aangeboden.

4.3.2.1. Maken van foto's/filmopnames van de leerlingen door de school:

De school of een cameraploeg maakt foto's, video- en televisieopnames van leerlingen tijdens verschillende evenementen in de loop van het schooljaar. Deze worden gebruikt voor hun communicatiekanalen (schoolwebsite, sociale media, ...) of om onze publicaties te illustreren. De school heeft daarvoor de individuele toestemming van je ouders nodig (zie toestemmingsformulier als bijlage). Indien de minderjarige leerling bekwaam geacht wordt dan is de toestemming van de bekwame leerling en zijn/haar ouders nodig. Indien de leerling meerderjarig is, wordt de toestemming door de meerderjarige leerling gegeven.

Indien je ouders hun keuze in de loop van het schooljaar willen wijzigen, nemen zij contact op met de directeur van de school, die hen een formulier ter ondertekening overhandigt.

4.3.2.2. Mediawijsheid leerlingen

Het is ook belangrijk mediawijsheid te creëren bij leerlingen. In het schoolreglement is vermeld dat toestemming moet worden gevraagd om foto's te maken/filmpjes te maken en toestemming om deze te gebruiken/verspreiden:

Zowel in de klas, op het schooldomein als tijdens buitenschoolse activiteiten mag je enkel foto's maken of filmen, met de uitdrukkelijke schriftelijke toestemming van de betrokken personen (bv. een leerkracht, een medeleerling, e.d.).

Naast de uitdrukkelijke toestemming om foto's te maken en te filmen, heb je de schriftelijke toestemming van de gefilmde of gefotografeerde personen nodig om deze foto's en beeldmateriaal te gebruiken, te verspreiden en te publiceren (bijvoorbeeld op sociale media).

4.3.3. Schoolactiviteiten

Indien er door de school foto's worden genomen/filmpjes worden gemaakt tijdens schoolactiviteiten waar ook derden kunnen op staan (bv. schoolfeest, eetfestijn, …), moet de school hierover informeren. Dit kan door bv. een boodschap zichtbaar uit te hangen (bv. in de inkom van de school, in de plaats waar de schoolactiviteit plaats heeft,…)/vermelden op inschrijvings- of deelnemingsformulier,…* waarop volgende moet worden vermeld:

- dat er foto's genomen worden/gefilmd wordt

- voor welk doel
- het kanaal van publicatie/verspreidingsvorm

Opgelet: bij het nemen van gerichte beelden:
- schriftelijke toestemming vragen voor nemen én voor het publiceren
- poseren is hetzelfde als toestemming geven voor het nemen van de foto MAAR niet voor het gebruiken of verspreiden ervan. Hiervoor moet je ook toestemming vragen. Opgelet met poseren door kinderen: zorg voor expliciete toestemming.

Maak ook afspraken met/informeer ook ouders en anderen over de regels die gelden bij het nemen van foto's/het maken van filmpjes,
Gerichte beelden: schriftelijke toestemming voor nemen en publiceren foto's/filmpjes. je kan dat opnemen bij het informeren (zie *). Zo neem je als school ook je verantwoordelijkheid op om hen te informeren. Wat zij verder doen, daar is school niet voor verantwoordelijk.

Er is geen toestemming vereist voor het nemen van foto's/maken van filmpjes als het gaat om foto's en filmpjes voor persoonlijke/huishoudelijk gebruik: de foto's staan enkel op jouw fototoestel/computer en je doet er verder niets mee behalve bekijken, afdrukken voor jezelf (niet-publiek), in album bewaren
Opgelet: als je deze foto's verspreidt of publiceert, heb je daar expliciet de toestemming voor nodig van iedereen op de foto/het filmpje. Anders pleeg je een inbreuk op het recht op afbeelding.

4.3.3.1. Maken van foto's/filmopnames door school van personeel

Gerichte beelden: toestemming nodig voor nemen en verspreiden/publiceren
Sfeerbeelden: Voor zulke beelden volstaat het dat je de betrokken personen inlicht over het feit dat dergelijke beelden zullen worden genomen, voor welk doel je dat doet en om welke publicatie het gaat.

Echter: de context moet steeds mee in de afweging worden genomen: er moet geval per geval worden bekeken of de privacy van personen aangetast kan worden.

4.3.4. Beveiligingsmaatregelen

Om een aantal discussies op voorhand in de kiem te smoren, wil de Privacycommissie ook enkele tips meegeven. Voor de publicatie van foto's op het internet kan gedacht worden aan volgende beveiligingsmaatregelen:

- Hou altijd rekening met de verleende toestemming
- Plaats niet zomaar alles online. Denk na over wat je op het internet zet. Gebruik geen beeldmateriaal dat compromitterend kan zijn voor de betrokken personen.
- Scherm specifieke pagina's met foto's af voor zoekmachines (zodat een zogenaamde indexering wordt tegengegaan),
- Plaats het materiaal op eigen sites met beperkte toegang
- Gebruik indien mogelijk wachtwoorden of een andere passende methode om een doelgroep af te bakenen,
- Beveilig machines en achterliggende databases tegen onbevoegde toegang door derden,
- Zorg ervoor dat een foto niet zomaar kan bewaard worden bv. via een klik met de rechtermuisknop.

En als het niet mogelijk is om toestemming te vragen? Zorg er dan voor dat je de beelden voldoende anoniem maakt.

BIJLAGEN

1. Formulier melden gegevenslek