vvsg Vereniging van Vlaamse Steden en Gemeenten

datum: 12 november 2024

[Sjabloon]

Richtlijnen informatieveiligheid en privacy voor mandatarissen

VVSG vzw • Bischoffsheimlaan 1-8 • 1000 Brussel • T +32 2 211 55 00
BIC GKCCBEBB • IBAN BE10 0910 1156 9604 • RPR Brussel BE 0451 857 573
info@vvsg.be • www.vvsg.be

vvsg

INHOUD[1]

[1] Dit sjabloon werd opgesteld in samenwerking met stad Leuven, stad Mechelen, stad Oostende, C-smart, Polis en VERA.

1. Toepassingsgebied

Deze richtlijnen zijn van toepassing op alle mandatarissen van [naam lokaal bestuur]. Extra waakzaamheid is vereist wanneer ze persoonsgegevens[2], vertrouwelijke of zeer vertrouwelijke gegevens ontvangen of verwerken.

Elke mandataris is persoonlijk verantwoordelijk voor de aan hem toevertrouwde persoons- en andere gegevens krachtens het beroepsgeheim, de geheimhoudingsplicht en de discretieplicht[3]. Bijzondere aandacht geldt voor de gegevens uit de Kruispuntbank Sociale Zekerheid (KSZ), het Rijksregister, het Centraal Strafregister en/of andere bronnen met gevoelige persoonsgegevens (bijvoorbeeld GAS boetes) of verkregen via het inzagerecht.

Dit document legt afspraken vast rond topics van informatieveiligheid en privacy.
Elk lokaal bestuur heeft de volgende wettelijke verplichtingen waaraan ze moet voldoen:

- Wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid en het toepassen van de minimale veiligheidsnormen;
- Decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer zoals gewijzigd bij het AVG-decreet;
- Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming), hierna 'AVG', met name artikel 1.1. dat bepaalt dat bij deze verordening regels worden vastgesteld betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en artikel 1.2. dat bepaalt dat deze verordening de grondrechten en de fundamentele vrijheden van natuurlijke personen beschermt en met name hun recht op bescherming van persoonsgegevens;
- Het decreet over het lokaal bestuur van 22 december 2017.
- Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

[Naam lokaal bestuur] heeft daarnaast de volgende verplichtingen waaraan medewerkers en mandatarissen moeten voldoen:

- Huishoudelijk reglement van [naam lokaal bestuur]
- ICT-code van [naam lokaal bestuur]
- Deontologische code van [naam lokaal bestuur]
- [andere]

[2] De Algemene Verordening Gegevensbescherming 2016/679 (EU) (AVG/GDPR) van 27 april 2016 en toepasselijke regelgeving(en) inzake privacy en gegevensbescherming zijn van toepassing.

[3] Zie ook 4.3. Verantwoordelijkheden

De wetgeving verplicht elk lokaal bestuur om in verhouding gepaste technische en organisatorische maatregelen te implementeren op gebied van informatieveiligheid, digitale veiligheid en privacy. Daarom is het van belang dat deze richtlijnen door elke mandataris goed nageleefd worden. Door goede naleving kan [naam lokaal bestuur] garanderen dat de vertrouwelijkheid, integriteit en beschikbaarheid van (persoons)gegevens niet geschonden wordt.

2. Doelgroepen

Deze afsprakennota is van toepassing op de volgende doelgroepen:

- Leden van het college van burgemeester en schepenen;
- Leden van de gemeenteraad;
- Leden van het vast bureau;
- Leden van de raad voor maatschappelijk welzijn (OCMW-raad);
- Leden van het bijzonder comité voor de sociale dienst (BCSD)

3. Digitale middelen[4]

3.1. Professioneel werken

De mandataris is professioneel in het gebruik van e-mail, intranet, internet, sociale media. Wat is niet toegelaten? (Niet limitatieve lijst)

- Berichten, die als een aantasting van iemands menselijke waardigheid kunnen beschouwd worden, doorsturen. Bijvoorbeeld berichten, die door de ontvanger, ervaren kunnen worden als racistisch, discriminerend (op basis van geslacht, seksuele geaardheid, godsdienst, afkomst, handicap, …), seksueel intimiderend, etc.
- Bestanden met aanstootgevende, pornografische of racistische inhoud consulteren, downloaden, openen of verspreiden. Zelfs niet indien het gaat om wettelijk toegelaten publicaties. De ICT-dienst blokkeert ongepaste sites zo veel mogelijk.
- Deelnemen aan kettingmails.
- Ontvangen e-mails systematisch doorsturen naar een elektronisch adres buiten de organisatie (bijvoorbeeld naar een privé e-mailadres).
- Gegevens in strijd met auteursrechten verspreiden of downloaden.
- Spelletjes, ontspanningsprogramma's, muziek, films, foto's, enz., downloaden of starten voor niet-professioneel gebruik.
- Bestaande veiligheidsmaatregelen of richtlijnen niet in acht nemen, omzeilen of neutraliseren, of proberen dit te doen. Bijvoorbeeld 'verboden' bestanden hernoemen om deze toch te kunnen raadplegen.
- Zich onrechtmatig toegang verschaffen tot de informaticasystemen van de organisatie.

[4] Zie ook ICT-code

- De goede werking van de informatiesystemen belemmeren of verhinderen.
- Op eender welke manier, ongeautoriseerd, vertrouwelijke persoons-, klant- of bedrijfsgegevens verspreiden.
- De vertrouwelijkheid en integriteit van de gegevens schenden of hun beschikbaarheid belemmeren.
- Foutieve informatie, om de organisatie of medewerkers in een slecht daglicht te plaatsen, bewust doorgeven.

3.2. E-mailgebruik

Enkel het gebruik van een officieel e-mailadres, met domeinnaam van het bestuur, wordt toegelaten. Dit e-mailadres wordt toegekend door de ICT-dienst volgens de standaard die geldt voor de personeelsleden van het lokaal bestuur. Op de website van het bestuur worden enkel de officiële e-mailadressen van de mandatarissen vermeld. Het automatisch doorsturen van e-mails naar een persoonlijk e-mailadres is niet toegelaten.

Het bestuur zal een elektronische mailbox ter beschikking stellen voor alle schepenen en raadsleden. Hierbij hoort een gebruikersnaam en wachtwoord dat strikt persoonlijk is voor gebruik. De schepenen en raadsleden kunnen hun wachtwoord zelf veranderen. Als het niet duidelijk is op welke manier dat moet, kan de dienst ICT hen bijstaan.

Voor het beveiligd delen van dossiers in het bestuur, zal een digitale omgeving [OneDrive/Sharepoint/Andere] ter beschikking worden gesteld die de schepenen en leden van het vast bureau kunnen gebruiken. Dossiers onderling doorsturen via e-mail wordt afgeraden. Inhoudelijke dossiers of informatie van het bestuur mogen niet worden doorgestuurd, ook niet versleuteld, naar privé mailboxen of niet gedeeld worden via onbeveiligde platformen zoals Dropbox, Google Drive.

Het e-mailadres met domeinnaam van het bestuur mag niet gebruikt worden om de nieuwsbrieven van de eigen politieke partij naar alle partijleden te sturen of om verkiezingsreclame naar inwoners te versturen.

3.3. Wachtwoorden

Álle wachtwoorden zijn strikt persoonlijk en worden niet gedeeld. Dit houdt in dat een mandataris enkel met zijn eigen gebruikersnaam en wachtwoord mag inloggen. De mandataris kiest een persoonlijk, sterk wachtwoord en volgt de tips en wachtwoordbeleid van de ICT-dienst.

Een wachtwoord mag nergens neergeschreven worden of bewaard worden op een fysieke plaats of in een document met de naam ‘paswoord’ of ‘wachtwoord’ erin. De mandataris vermijdt dat een derde toegang krijgt tot alle informatie (bedrijfsinformatie en/of persoonsgegevens) waar hij/zij toegang tot heeft (bijvoorbeeld via netwerktoegang, e-mails, gebruikte applicaties). Dit is extra belangrijk bij gebruik van tablets, laptops, externe gegevensdragers en andere mobiele toestellen.

3.4. Netwerk

Wanneer relevant voor zijn functie krijgt de mandataris toegang tot een specifiek gedeelde van het interne netwerk:
[duid aan welke van de twee naar gelang het beleid van het lokaal bestuur]

- [Optie 1] mits gebruik van een professioneel toestel. Het wachtwoord van het interne netwerk wordt aan de ICT-dienst gevraagd en mag in geen geval doorgegeven worden aan derden.

  Via een privé toestel kan enkel verbonden worden met het externe gastennetwerk. Ook verbinding via vaste kabel met het internet netwerk is verboden.

- [Optie 2] En/of met een privé toestel voor het uitvoeren van professionele taken.

  Een mandataris die toegang wil op het netwerk of de applicaties van de organisatie via een ander toestel dan het toestel voorzien door de organisatie, garandeert dat beveiligingssoftware hierop geïnstalleerd en up-to-date is. De dienst ICT kan verifiëren of de configuratie en veiligheidssoftware van een toestel conform is. In geval van afwijkingen, brengt de dienst ICT verslag uit aan het informatieveiligheidsteam.

Het netwerk van de organisatie is standaard beveiligd. Beveiligingssoftware (antivirus, antispam, firewall) op professionele toestellen wordt niet gewijzigd of uitgeschakeld.

Als je via andere (gratis) aangeboden verbindingen werkt (hotspots, wifi, hotels, ..), is dit niet altijd het geval. Mandatarissen beperken het werken op andere (gratis) aangeboden verbindingen tot het absolute minimum. Er worden geen persoonsgegevens of andere gevoelige informatie via een onbeveiligde verbinding of een verbinding waarvan de veiligheid onzeker is, geraadpleegd.

3.5. Software

Voor elke vorm van digitale handelingen via het professionele toestel maakt de mandataris uitsluitend gebruik maken van software die door de dienst ICT geïnstalleerd is. Indien er toch nood is aan andere software, wordt contact opgenomen met de dienst ICT.

Je transfereert geen software, die door de organisatie aan jou ter beschikking wordt gesteld, over naar eigen apparatuur, behoudens toestemming van ICT. Intellectuele eigendomsrechten moeten steeds gerespecteerd worden.

[Indien er elektronisch vergaderd wordt, zal de toepassing Microsoft Teams gebruikt worden. Elke gebruiker heeft een individuele gebruikersnaam en wachtwoord om hiermee te werken. Het gebruik van Microsoft Teams is zowel op een professioneel als op een privé toestel toegestaan.]

3.6. Hardware

Het bestuur kan indien nodig externe media beschikbaar stellen in bruikleen voor de periode van het mandaat. Dit gebruik zal worden geregistreerd door middel van een inventaristool, en na het beëindigen van het mandaat dienen deze ook integraal ingeleverd te worden[5]. Met het aanvaarden van de externe media, wordt akkoord gegaan met de ICT-code en deze richtlijnen.

De door [lokaal bestuur] ter beschikking gestelde toestellen worden niet gebruikt door derden, tenzij onder toezicht van een medewerker van de organisatie, bijvoorbeeld in het kader van een presentatie of opleiding.

3.7. Data opslag en back-up

De dienst ICT zorgt voor een automatische back-up van alles wat gebruikt wordt via de netwerkinfrastructuur (netwerkdrives en lokale SharePoint) van de organisatie.

Er wordt geen back-up gemaakt door de organisatie van gegevens die lokaal bewaard worden op (mobiele) toestellen. De mandataris bewaart geen persoonsgegevens of vertrouwelijke informatie lokaal op het toestel. Indien dit toch gebeurt, kopieer de informatie dan onmiddellijk naar het netwerk en verwijder ze definitief van de lokale harde schijf.

Het wordt ten zeerste afgeraden gebruik te maken van publiek aangeboden kanalen (bijvoorbeeld Dropbox), onbeveiligde of onvoldoende beveiligde platformen om gevoelige of vertrouwelijke gegevens te bewaren of uit te wisselen. Wanneer hierop aangedrongen wordt, moet de ICT-dienst eerst gecontacteerd worden.

3.7.1. Dossiers[6]

Dossiers zijn eigendom van het bestuur en zijn vertrouwelijk, ze mogen niet gedeeld worden zonder toestemming en zijn enkel beschikbaar voor de bevoegde personen en niet voor derden. Het is ten strengste verboden zonder voorafgaand akkoord van het bestuur:

- Digitale kopieën te maken van dossiers.
- Digitale/analoge dossiers door te mailen naar eigen mailadressen.
- Persoonsgebonden dossiers te printen of op te slaan op een andere drager.

Sociale dossiers vallen onder de elektronische terbeschikkingstelling. Sociale verslagen verbonden aan agendapunten dienen vanaf de verzending van de oproeping ter beschikking worden gehouden voor de leden van het BCSD.

---

[5] Zie ook bijlagen A en B
[6] Zie ook 4.2. Inzagerecht

Bij dossiers die raken aan de persoonlijke levenssfeer wordt altijd de afweging gemaakt of de vraag om inzage in verhouding staat tot de bescherming van de persoonlijke levenssfeer van de betrokkene.

3.8. USB-sticks of andere mobiele opslagmedia[7]

De leden van de doelgroep plaatsen geen vertrouwelijke gegevens en/of persoonsgegevens op en USB-stick of andere mobiele drager en beperken over het algemeen het gebruik hiervan. Indien ze bestanden willen overplaatsen naar hun toestel, scannen ze de drager eerst op mogelijke bedreigingen. Een rondslingerende USB-stick waarvan de oorsprong onbekend is, wordt nooit in een toestel gestoken maar bezorgd aan de dienst ICT.

Printen via een privé USB-stick is een beveiligingsrisico en daarom verboden.

4. Rechten en plichten van de mandataris m.b.t. informatieveiligheid

4.1. Privacy

[Naam lokaal bestuur] verzamelt, bewaart en verwerkt gegevens van de mandatarissen van de organisatie. Deze gegevens worden opgenomen en bewaard in bestanden, zowel op papier als digitaal, en worden enkel gebruikt in het kader van personeelsadministratie/loonadministratie en de vlotte werking van de bestuursorganen.

De houder van de bestanden is het bevoegd bestuursorgaan, College van Burgemeester & Schepenen of Vast Bureau, [adres]. De verantwoordelijke voor het dagelijks bestuur is de Algemeen Directeur.

Elke mandataris heeft het recht om zijn/haar gegevens op te vragen. Dit kan via de personeelsdienst. Bij vragen of bezorgdheden over de verwerking van persoonsgegevens kan de functionaris voor gegevensbescherming (DPO) gecontacteerd worden via [emailadres DPO]. In tweede instantie kan de Vlaamse Toezichtcommissie (VTC) bevraagd worden.

4.2. Inzagerecht

Een raadslid staat in voor de democratische controle op de gemeente en het OCMW en kan mee beleid maken. Het is daarbij belangrijk om de juiste gegevens te hebben. Daarom hebben raadsleden een dubbel inzagerecht:

[7] Zoals SD-kaarten, CD-roms, DVD's

4.2.1. Specifiek inzagerecht

Specifiek voor het voorbereiden van de vergadering worden alle documenten tijdig ter beschikking gesteld van de raadsleden. Zodra de agenda bezorgd wordt, kunnen de dossiers worden ingekeken, zowel op papier als digitaal.

4.2.2. Algemeen inzagerecht

Een raadslid kan daarnaast ook inzage vragen in alle dossiers, stukken en akten met betrekking tot het bestuur van de gemeente en het OCMW. Er is geen onderscheid tussen papieren documenten of digitale informatie. Een bestuursdocument wordt ruim gedefinieerd: de drager, in welke vorm ook, van informatie waarover een instantie beschikt. Alle informatie waarover de lokale overheid beschikt, kan worden opgevraagd. Ook documenten van derden vallen hieronder.

Inzage betekent ook een recht op afschrift of kopie van de dossiers, stukken en akten. [Naam lokaal bestuur vraagt hiervoor de vergoeding van …]. De modaliteiten waaronder afschriften en kopieën worden verkregen zijn opgenomen in het huishoudelijk reglement van de gemeente- en OCMW-raad van [naam lokaal bestuur]. Afschrift kan op papier, maar kan ook digitaal gevraagd worden.

Bij inzagerecht zijn er volgende uitzonderingen:

- Stukken die niet "af" zijn, worden uitgesloten van inzage tot ze wel "af" zijn. Deze uitzondering geldt enkel voor het stuk waaraan nog gewerkt wordt, niet voor eventuele andere stukken uit hetzelfde dossier die wel al "af" zijn.
- Persoonlijke documenten (bijvoorbeeld notities ter voorbereiding van een verslag) kunnen niet ingekeken worden door raadsleden.
- Inzage kan enkel gevraagd worden voor bestaande stukken. Een raadslid kan dus niet eisen dat een nieuw document opgesteld wordt. Dat kan enkel als de raad dit toestaat.
- Raadsleden hebben voor de gemeente geen inzage in de stukken die verband houden met de taken van algemeen belang, zoals bijvoorbeeld het bevolkings- of strafregister.
- In het OCMW hebben raadsleden geen recht op afschrift (of kopie) voor de dossiers die betrekking hebben op de persoonlijke levenssfeer van cliënten van het OCMW en van hun onderhoudsplichtigen.

.

4.3. Verantwoordelijkheden

Gemeente- en OCMW-raadsleden zijn steeds persoonlijk verantwoordelijk voor de uitoefening van hun inzagerecht en het gebruik van de informatie die ze op basis daarvan verkregen hebben. De informatie wordt enkel verkregen in de hoedanigheid van raadslid en mag dan ook enkel in de uitoefening van het mandaat worden aangewend.

Als tegenhanger voor het ruime inzagerecht moeten raadsleden vertrouwelijke gegevens uit de openbaarheid houden. Volgende plichten gelden:

- Het beroepsgeheim wordt opgelegd door art. 458 van het Strafwetboek, waardoor inbreuken strafrechtelijk vervolgd kunnen worden (ook al is er geen schade bij derden). Het decreet lokaal bestuur bevestigt dat dit beroepsgeheim van toepassing is op zowel lokale politici als personeelsleden. Naast een mogelijke strafsanctie kan een inbreuk op het beroepsgeheim ook schade berokkenen en aanleiding geven tot een schadevergoeding.

- Het decreet lokaal bestuur legt ook de geheimhoudingsplicht op. Wat een 'geheim' is, wordt niet gedefinieerd. Er wordt aangenomen dat dit voor raadsleden gaat om informatie die:
    - ze enkel kennen door de uitoefening van hun mandaat of functie;
    - niet gaat over publieke feiten en dus niet gekend is door derden;
    - toevertrouwd of vastgesteld werd in het kader van een vertrouwensrelatie (bijvoorbeeld een hulpverleningsvraag).

- Discretieplicht: daarbij gaat het om informatie die:
    - het raadslid enkel kent door de uitoefening van zijn mandaat of functie;
    - niet over publieke feiten gaat en dus niet gekend is door derden.

  In tegenstelling tot geheimhoudingsplicht gaat niet alleen om informatie die wordt verkregen in het kader van een vertrouwensrelatie. Raadsleden hebben de plicht om bij het communiceren voorzichtigheid te hanteren. Wanneer er door hun toedoen zaken uit de beslotenheid gehaald worden, die niet publiek gemaakt kunnen worden, dan maakt de politicus een fout die eventueel schade berokkent en die aanleiding kan geven tot een schadevergoeding.

- Deontologische plichten: [Naam lokaal bestuur] heeft een deontologische code voor de mandatarissen. Het geeft een belangrijk kader waarbinnen elk raadslid veilig kan werken. Ook de samenstelling, werking en bevoegdheden van de deontologische commissie is erin opgenomen.

Mandatarissen verbinden zich ertoe enkel in opdracht van de organisatie te handelen bij het verwerken van gegevens. Ze verschaffen zich enkel toegang tot de gegevens, die noodzakelijk zijn voor het uitvoeren van de aan hen toevertrouwde opdracht(en). Ze vertrouwen gegevens, waarvan ze kennis nemen, enkel toe aan anderen in de mate dat dit voor de uitvoering van hun opdracht noodzakelijk is en op voorwaarde dat deze persoon (aan wie de gegevens kenbaar gemaakt worden) gemachtigd is er kennis van te nemen. Elke mandataris is verantwoordelijk voor zijn/haar communicatiegedrag.

4.4. Veilige raadpleging van elektronische documenten

Mandatarissen kunnen dossiers op een veilige en betrouwbare wijze inkijken. Bij dossiers die niet meer relevant zijn, wordt de toegang ingetrokken.

Mandatarissen hebben geen toegang tot de bestaande mappenstructuur van de administratie. Een aparte mappenstructuur is wel mogelijk. Daarnaast hebben ze ook geen toegang tot softwarepakketten van de diensten, tenzij dit noodzakelijk is het voor

het uitvoeren van hun mandaat en dit op een veilige en correcte manier mogelijk gemaakt is via rechten- en toegangenbeheer.

5. Fysieke toegang

[Zelf aan te vullen, denk aan sleutelbeheer, toegang tot bepaalde ruimtes, reserveren van zalen]

6. Goede praktijken

Mandatarissen passen onderstaande goede praktijken toe om het risico op een gegevenslek te minderen.

- Plaats een mobiel toestel in sluimerstand wanneer het niet gebruikt wordt of onbewaakt is.
- Vergrendel de computer via ⊞ + L bij het verlaten van de werklocatie.
- Documenten met gevoelige informatie worden nergens onbewaakt achtergelaten, ook niet op een printer.
- Zorg ervoor dat bij het werken in aanwezigheid van derden, op een publieke plaats, er geen toegang is tot gevoelige informatie of persoonsgegevens. Voorkom dat iemand kan meelezen.
- Alle gevoelige papieren of elektronische documenten moeten zich achter slot bevinden in de daartoe bestemde kasten bij het verlaten van de werkruimte.
- Wees bewust van het hoge risico op cybercriminaliteit en andere pogingen om toegang te krijgen tot vertrouwelijke informatie of persoonsgegevens. Informeer bij de ICT-dienst over mogelijke bewustmakingscampagnes of trainingen om de weerbaarheid m.b.t. cyberveiligheid te verhogen.

7. Controle

[Lokaal bestuur] respecteert de privacy van de mandatarissen. Toch zullen een aantal controlemaatregelen genomen worden. Dit om de goede werking van de apparatuur en naleving van regelgeving te verzekeren. De Algemeen Directeur, ICT-dienst en functionaris voor gegevensbescherming (DPO) waken over de naleving.

Bij controles of screening door middel van aangepaste software worden in eerste instantie inhoudelijke gegevens niet ingekeken. In de mate zij zouden ingekeken moeten worden, wordt de vertrouwelijkheid door de ICT-dienst gegarandeerd.

De functionaris voor gegevensbescherming (DPO) zal controles uitvoeren op de naleving van toepasselijke wet- en regelgeving, gedragscodes, richtlijnen, afspraken, enzoverder in het kader van informatieveiligheid en gegevensbescherming.

Bij vermoeden van misbruik of overtredingen wordt de algemeen directeur ingelicht. Hij geeft opdracht om een onderzoek in te stellen. In dat geval kan bijvoorbeeld het e-mail- en internetgebruik van een medewerker nader bekeken worden. De controles zullen beperkt zijn en evenredig met de aard van het vermoede misbruik. Doorgedreven

onderzoek, waarbij alle gegevens en inhoud van alle verrichtingen via e-mail en internet onderzocht worden, is enkel mogelijk bij aantoonbaar en ernstig vermoeden van misbruik.

Het bestuur is bevoegd om alle richtlijnen te controleren samen met de functionaris gegevensbescherming. Wanneer misbruik of inbreuken op deze afspraken worden vastgesteld, is het bestuur door wetgeving verplicht dit te melden bij de Gegevensbeschermingsautoriteit of de Vlaamse Toezichtcommissie. Het niet naleven van afspraken kunnen administratieve en/of strafrechtelijke sancties tot gevolg hebben. Het niet inleveren van gemeentelijke eigendommen kan een officiële klacht van diefstal tot gevolg hebben.

8. Meldplicht van inbreuken, risico's en gegevenslekken

Elke mandataris is verplicht, waar nodig, gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht ervan.

De mandataris meldt inbreuken, of een vermoeden ervan, zo snel mogelijk aan het informatieveiligheidsteam, via […].

Elk (mogelijk) probleem met het netwerk, alle misbruik van de internet- en e-mailfunctionaliteiten (virussen, pogingen tot intrusie of hacking), ongeacht of dit op het niveau van de centrale computers, het netwerk, de lokale computers of de software is, worden zo snel mogelijk gemeld aan Dienst ICT. Dienst ICT verwittigt de functionaris voor gegevensbescherming (DPO). De mandataris neemt de gepaste geheimhouding in acht ten opzichte van anderen met betrekking tot (vermoedelijke) inbreuken, risico's en problemen.

Bij diefstal van een toestel dat informatie bevat, waarvan [lokaal bestuur] eigenaar is,, doet de mandataris aangifte bij de politie en neemt hij/zij zo snel mogelijk contact op met de ICT- dienst. Ze gaan samen na of er effectief sprake is van een inbreuk met betrekking tot persoonsgegevens (gegevenslek). De ICT-dienst verwittigt de functionaris voor gegevensbescherming (DPO).

Bijlage A:

Als nieuwe mandataris starten bij de organisatie – checklist

Fysieke toegang	
	Sleutel(s)
	Badges
	Code
	Parkeermogelijkheid
	Vergaderzaal boeken
	Rondleiding
Toestellen	
	Laptop
	Tablet
	Smartphone
	Toegang tot printer
Software en accounts	
	Account + wachtwoordbeleid of MFA
	E-mailadres en mailbox
	Toegang tot intranet
	Toegang tot notuleringssoftware
	Relevante toegangsrechten
Opleiding	
	Richtlijnen informatieveiligheid
	ICT-code

	Deontologische code
	Huishoudelijk reglement
	Informatie en opleidingen van VVSG voor mandatarissen
	Cyber security awareness
Privacy	
	Toestemming voor het publiceren van naam, e-mailadres, titel mandaat en partij op de website van het bestuur.
	Toestemming voor het nemen en publiceren van een foto op de website

Bijlage B:

Als mandataris de organisatie verlaten - checklist

Fysieke toegang	
	Sleutel(s) terugbezorgd
	Badges terugbezorgd
	Code verwijderd
Toestellen	
Laptop	
	Persoonlijke bestanden verwijderd of overgezet
	Dossiers terugbezorgd aan het bestuur
	Laptop terugbezorgd
Tablet	
	Persoonlijke bestanden verwijderd of overgezet
	Dossiers terugbezorgd aan het bestuur
	Tablet terugbezorgd
Smartphone	
	Persoonlijke bestanden verwijderd of overgezet
	Smartphone terugbezorgd
Andere	
	Toegang tot printer verwijderd
	Headset, scherm, toetsenbord, muis, … terugbezorgd
Software en accounts	
	Account verwijderd na […]
E-mailadres en mailbox	
	Out-of-office ingesteld
	Persoonlijke e-mails verwijderd

	Relevante e-mails bewaard op intranet of doorgestuurd naar administratie
	Mailbox verwijderd na […]
Gegevens	
	Dossiers (op papier en op andere dragers) terugbezorgd aan het bestuur of correct gearchiveerd
	Documentatie met persoonsgegevens versnipperd of terugbezorgd aan de bevoegde administratie
	Gegevens verkregen via inzagerecht verwijderd
	Geïnformeerd over verbod op verder gebruik en verwerking van persoonsgegevens en vertrouwelijke informatie verkregen door uitvoering van mandaat
	Geïnformeerd over blijvende plichten inzake informatie verkregen door uitvoering van mandaat
	Gegevens van de mandataris op de website verwijderd