Dienstnota van de provinciegriffier

Nummer:	**DAB - 24 - 2022**
Onderwerp:	**Informatieveiligheid: veilig en correct omgaan met persoonsgegevens en ICT-middelen**
Contactgegevens:	Katty Scholdis - informatieveiligheid@provincieantwerpen.be
Samenvatting:	Deze nota geeft een aantal concrete voorschriften om op een verantwoorde en consistente manier om te gaan met informatie, in lijn met de bestaande wetgeving en de verwachtingen van onze klanten en de organisatie.
Van toepassing op	Medewerkers van de binnen- en buitendiensten en volgende APB's en EVAP's: APB PVM / APB POA (niet-gesubsidieerd personeel) / APB CVST APB PRZ / APB PRDS / APB TPA / APB WAR APB PIH APB PSES / APB PDA / APB GKC / APB KMPC / APB HH / APB HC EVAP AK / EVAP PSRN / EVAP PRLB / EVAP SKL / EVAP PV

Deze dienstnota treedt in werking op **20/06/2022**

Deze dienstnota vervangt dienstnota DAB–24–2021

Inleiding

Waarom een dienstnota over informatieveiligheid?

Als organisatie verzamelen en verwerken we heel wat informatie bij de provincie Antwerpen. Deze informatie is kostbaar en we verwachten dat we er altijd en van overal aan kunnen. Daarom vraagt de bescherming en beschikbaarheid van deze informatie de nodige aandacht.

We nemen enerzijds een aantal organisatorische maatregelen. We stellen bijvoorbeeld procedures op voor het goedkeuren van bepaalde aanvragen, het beheren van contactgegevens en het archiveren van afgewerkte dossiers.

Anderzijds implementeren we ook een aantal technische maatregelen. Denk maar aan het voorzien van toegangscontrole tot de gebouwen en ICT-systemen, het gebruik van antivirustoepassingen en het nemen van back-ups voor het geval er toch iets misloopt.

Maar ook jij kan jouw steentje bijdragen. Jij komt immers dagelijks in contact met informatie. Jouw collega's en onze klanten verwachten dat je hier als een goede huisvader mee omgaat. Bovendien ben je bij het verwerken van deze informatie gebonden aan de bestaande wetgeving, zoals de privacywetgeving, het auteursrecht enzovoort.

Vandaar deze dienstnota. Met deze nota geven we een aantal concrete voorschriften om op een verantwoorde en consistente manier om te gaan met informatie, in lijn met de bestaande wetgeving en de verwachtingen van onze klanten en de organisatie. Deze nota kan je daarom beschouwen als een aanvulling op de algemene afspraken in de deontologische code en het arbeidsreglement (meer bepaald 'bijlage 4 – IT-policy').

Deze dienstnota geldt eveneens tijdens het telewerken. We verwachten dat je de principes rond gegevensbescherming en de manier waarop je met de ICT-middelen omgaat ook tijdens het telewerken toepast. Laat werkdocumenten met persoonsgegevens of andere (gevoelige) gegevens niet rondslingeren en vergrendel je mobiele apparaten bij het verlaten van je werkplek.

Op wie is dit van toepassing?

Deze dienstnota geldt voor de medewerkers van alle provinciale entiteiten – binnendiensten, buitendiensten, APB's en EVAP's.

Ook externe medewerkers, leveranciers en andere personen die gebruik maken van provinciale ICT-middelen leven deze dienstnota na. Dit wordt contractueel opgenomen of ze ondertekenen hiervoor een integriteitsverklaring.

Hoe is de dienstnota opgebouwd?

Deze dienstnota geeft een aantal voorschriften om veilig om te gaan met persoonsgegevens (privacy) en met ICT-middelen (security), en laat je weten op welke manier toezicht kan worden uitgeoefend hierop.

Privacy – Veilig omgaan met persoonsgegevens

Wij als organisatie hechten grote waarde aan het correct beschermen van de gegevens die zij verwerkt, in het bijzonder persoonsgegevens. Daarom willen wij vastleggen op welke wijze persoonsgegevens moeten beschermd worden, welke verantwoordelijkheden hiervoor zijn toegewezen en welke prioriteiten wij hanteren voor de bescherming van persoonsgegevens.

Wij doen graag een beroep op iedereen die betrokken is bij de elektronische en papieren verwerking om samen, vanuit één gemeenschappelijke visie, de verwerking van persoonsgegevens correct te laten verlopen.

De richtlijnen in dit hoofdstuk zijn van toepassing voor de gehele levensduur van alle informatie binnen de provincie Antwerpen: van het verkrijgen tot de uiteindelijke verwijdering van de informatie.

Tip: Heb je twijfels over een bepaalde verwerking? Vraag dan advies aan informatieveiligheid@provincieantwerpen.be.

Begrippen

De AVG gebruikt een aantal begrippen die we kort toelichten:

- 'AVG': afkorting van Algemene Verordening Gegevensbescherming. Vaak wordt ook de Engelstalige afkorting 'GDPR' ('General Data Protection Regulation') gebruikt.
- 'Persoonsgegevens': alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, zowel directe informatie (bv. naam) als informatie die naar een bepaalde persoon te herleiden is (bv. combinatie van woonplaats en leeftijd). Gegevens van overleden personen of van organisaties zijn geen persoonsgegevens volgens de AVG (maar de gegevens van hun werknemers zijn wel persoonsgegevens).
- 'Verwerking': alle handelingen die een organisatie kan uitvoeren met persoonsgegevens, van verzamelen tot en met vernietigen, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, wijzigen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, wissen en vernietigen van gegevens .
- 'DPO': De provincie Antwerpen is als overheidsbedrijf verplicht om een DPO ('data protection officer') aan te stellen. Dit is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de Algemene verordening gegevensbescherming (AVG).
- 'Verwerkersovereenkomst': Indien we beroep doen op een derde partij maken we afspraken over hoe ze moeten omgaan met onze persoonsgegevens.
- 'Verwerkingsregister': een gedocumenteerd overzicht van alle activiteiten waarbij persoonsgegevens worden verwerkt.
- 'Datalek': We spreken van een datalek van zodra persoonsgegevens dreigen ongeoorloofd openbaar te worden gemaakt, verloren te gaan, vernietigd of gewijzigd te worden. Het is hier dus niet nodig dat er effectief data gebruikt wordt door een derde. Het feit dat een onbevoegde toegang heeft tot de gegevens is voldoende.

Basisprincipes

Wil je in de uitvoering van je job persoonsgegevens verwerken, dan moet je ervoor zorgen dat deze verwerking voldoet aan de volgende basisprincipes, die we in de volgende paragrafen verder toelichten:

- Rechtsgrond van de verwerking
- Doelbinding
- Minimale gegevensverwerking (proportionaliteit)
- Juistheid
- Beperkte bewaartermijn
- Integriteit en vertrouwelijkheid
- Verantwoordingsplicht

Rechtsgrond van de verwerking

Je mag niet zomaar persoonsgegevens verwerken. Je moet elke verwerking kunnen koppelen aan één van de volgende zes rechtsgronden.

- De betrokkene heeft de provincie Antwerpen **toestemming** gegeven voor een of meer specifieke doeleinden (bv. toesturen van een nieuwsbrief).

  Ter info: Toestemming is in de AVG aan heel wat voorwaarden verbonden. Niet elke toestemming verkregen voor de inwerkingtreding, blijft geldig.

- De provincie Antwerpen moet een **overeenkomst** met de betrokkene nakomen of is van plan om een overeenkomst met die partij te sluiten (bv. aankoop van een product).
- De provincie Antwerpen moet deze verwerking doen op basis van een **wet of decreet** (bv. personeelsgegevens verwerken voor afdrachten sociale zekerheid).
- De verwerking staat niet specifiek in een wet maar vloeit voort uit een door de wet opgelegde taak, ook wel gekend als '**taak van algemeen belang**' (bv. stuurgroepen organiseren).
- De provincie Antwerpen heeft een **gerechtvaardigd belang** (bv. het voorzien van een 'wie is wie' op intranet om het intern communicatieproces vlot te laten verlopen).

  Let op: Dit is een belangenafweging en mag enkel maar gebruikt worden in samenspraak met de DPO.

Hoe passen we dit toe bij de provincie Antwerpen?

Bij iedere nieuwe registratie van een activiteit in het verwerkingsregister, wordt er gevraagd naar een rechtsgrond.

Tip: Kan je geen rechtsgrond vinden voor een bepaalde verwerking? Stel dan deze vraag aan informatieveiligheid@provincieantwerpen.be .

Doelbinding

Gebruik gegevens alleen voor het doel waarvoor je ze hebt verkregen.

Bijvoorbeeld: gegevens opgevraagd voor een subsidieaanvraag mogen niet gebruikt worden om een nieuwsbrief te versturen.

Hoe passen we dit toe bij de provincie Antwerpen?

Bij iedere nieuwe registratie van een verwerkingsactiviteit in het verwerkingsregister, wordt er gevraagd naar doeleinden.

Tip: vraag je af waarom je die verwerking doet. Het antwoord daarop is het doeleinde.

Minimale gegevensverwerking (proportionaliteit)

Je mag uitsluitend de gegevens verwerken die noodzakelijk zijn om het beoogde doel te bereiken, dus enkel **het strikte minimum**.

Bijvoorbeeld: om een nieuwsbrief te versturen is enkel het e-mail adres (en eventueel de naam) nodig. Het postadres, telefoonnummer of geboortedatum mogen in dit kader niet worden opgevraagd.

Hoe passen we dit toe bij de provincie Antwerpen?

Bij de opstart van een nieuw project wordt er verwacht dat je rekening houdt met de privacyaspecten die hier bij komen kijken. We verwachten dat je tijdig advies vraagt aan de DPO.

Tip: Denk goed na bij elke nieuwe verwerking. Welke gegevens hebben we echt nodig? Welke gegevens gaan we hiervoor gebruiken? Gegevens verzamelen omdat ze misschien ooit nog van pas zullen komen, kan niet volgens de regels van de AVG.

Juistheid

De gegevens moeten juist zijn en zo nodig worden bijgewerkt.

Hoe passen we dit toe bij de provincie Antwerpen?

Via de provinciale website hebben alle burgers en personeelsleden een formulier waarmee ze het recht hebben om een verzoek tot verbetering in te dienen, de provincie zal hier gevolg aan geven binnen de 30 dagen (zoals wettelijk voorgeschreven). Die wijziging kan gaan over naam, adres, woonplaats, emailadres, telefoonnummer, aantal kinderen ten laste, nummerplaat, enzovoort.

Beperkte bewaartermijn

De gegevens mogen niet langer bewaard worden dan noodzakelijk is voor de verwezenlijking van de doelen.

Bijvoorbeeld: dossiers inzake subsidies die de dienst ontvangt van Europa worden 20 jaar bewaard (zoals bepaald in het informatiebeheersplan).

Hoe passen we dit toe bij de provincie Antwerpen?

De bewaartermijnen worden in kaart gebracht door de provinciale archivaris in de informatiebeheersplannen. Het langer bewaren van persoonsgegevens kan gerechtvaardigd worden met het oog op archivering in het algemeen belang, voor historisch of wetenschappelijk onderzoek of voor statistische doeleinden. Meer informatie hierover is terug te vinden in de toolbox informatiebeheer.

Integriteit en vertrouwelijkheid

De gegevens moeten volgens een afdoend veiligheidsniveau worden verwerkt door gebruik te maken van passende, technische en organisatorische maatregelen.

Bijvoorbeeld: toegangsbeheer, gebruikersrollen, encryptie, logging, enzovoort.

Hoe passen we dit toe bij de provincie Antwerpen?

Bij de opstart van een nieuw project wordt er verwacht dat je de nodige maatregelen treft om de persoonsgegevens te beschermen. We verwachten dat je tijdig advies vraagt aan de DPO.

Verantwoordingsplicht

De AVG-regels dwingen ons om goed na te denken over hoe onze organisatie persoonsgegevens verwerkt en beschermt. De AVG legt de verantwoordelijkheid bij ons als organisatie om aan te tonen dat we aan de privacyregels voldoen.

Hoe passen we dit toe bij de provincie Antwerpen?

Deze nota dekt alvast een deel van onze verantwoordingsplicht. Concreet verwachten we van jou:

- Jaarlijkse herziening van de verwerkingsregisters.
- Juiste verwijzing naar de privacyverklaring op alle invulformulieren.
- Bij het afsluiten van een nieuw contract/verlenging van een contract, verwijzen naar de nodige geheimhoudingsclausules en een verwerkersovereenkomst afsluiten indien nodig.
- Opgestelde procedures volgen om ervoor te zorgen dat de informatie beschermd blijft.
- Melden van potentiële datalekken die je tegenkomt (zie dienstnota 'Incidenten policy (DAB-23)').
- Meewerken aan een verzoek van een burger indien nodig (in het kader van uitoefening van rechten van betrokkenen).

Security – Veilig omgaan met ICT-middelen

Bij het uitvoeren van onze taken maken we gebruik van een aantal ICT-middelen om informatie te verwerken, zoals digitale bestanden, software en hardware. Hierboven gaven we aan waarom het belangrijk is om deze verwerkingen op een veilige manier te doen. Daarom neemt het departement ICT een aantal technische maatregelen om deze te beschermen, denk maar aan de antivirustoepassing, firewall, antispamfilter, versleuteling van harde schijven enzovoort.

Toch blijken technische maatregelen alleen niet te volstaan, getuige hiervan de regelmatige berichtgeving in de media over cyberaanvallen en -diefstallen. Vaak ligt een menselijke fout aan de oorzaak van dergelijke incidenten. Daarom geven we in dit hoofdstuk enkele concrete richtlijnen die je helpen om op een veilige manier om te gaan met de ICT-middelen die je dagelijks gebruikt.

Begrippen

Met de richtlijnen in de volgende paragrafen willen we ons wapenen tegen een aantal internetdreigingen. We sommen hier een aantal vormen op:

- Hacker: iemand die binnendringt in een ICT-systeem, zoals een pc of server, meestal met de bedoeling om informatie te stelen of onbruikbaar te maken.
- Ongewenste (e-mail)berichten:
    - Spam: ongevraagde reclameboodschappen die meestal verstuurd worden via e-mail.
    - Phishing: berichten die 'vissen' naar jouw gegevens, zoals aanmeldgegevens (gebruikersnaam en wachtwoord), bankgegevens, contactgegevens, enzovoort. Ze worden meestal verstuurd via e-mail, maar soms ook via social media of SMS.
- Malware: afkorting van 'malicious software' en dus de verzamelnaam van alle 'kwaadaardige software' waaronder computervirussen. De verspreiding gebeurt meestal via e-mailberichten die een met malware besmette bijlage bevatten of die je doorverwijzen naar een besmette website die ongemerkt de kwaadaardige software op je PC installeert.
    - Ransomware: specifieke vorm van malware die je pc (of een heel computernetwerk) gijzelt en losgeld ('ransom') vraagt om hem weer vrij te geven.
    - Backdoor: vele soorten malware laten een 'achterdeur' open op jouw pc zodat de hacker hem vanop afstand kan uitlezen (bv. om aanmeldgegevens of bankgegevens te stelen) of manipuleren (bv. om andere pc's aan te vallen).

Basisprincipes

Als provinciale medewerker ga je veilig en correct ('als een goede huisvader') om met de provinciale ICT-middelen. Algemeen betekent dit:

- Gebruik de middelen op een wettelijke manier met respect voor auteursrecht en privacy. Gebruik geen provinciale ICT-middelen om illegale informatie of boodschappen te verspreiden met als doel te discrimineren, intimideren, pesten, stalken, spammen, phishen, hacken enzovoort. Gebruik de middelen ook niet om websites te bezoeken die dergelijke boodschappen verkondigen of faciliteren.
- Gebruik de ICT-middelen niet op een manier die de provinciale ICT-infrastructuur kan aantasten. Download of stream bijvoorbeeld niet voortdurend bestanden van het internet en probeer de getroffen veiligheidsmaatregelen niet uit te schakelen of te omzeilen.
- Wees steeds op je hoede bij onverwachte e-mailberichten, telefoonoproepen of social media berichten. Dergelijke berichten kunnen een poging zijn om jouw pc te hacken of met een virus te besmetten. Controleer hyperlinks en bijlagen vooraleer je ze opent. (Hoe je dit doet vind je verder in deze nota terug.)

- Verwittig de ICT-servicedesk onmiddellijk bij (het vermoeden van) een ICT-incident (zoals diefstal of verlies van een laptop, misbruik van aanmeldingsgegevens, poging tot hacking, malwarebesmetting, onbeschikbaarheid van een ICT-applicatie, enzovoort). Ook bij vragen over ICT-security kan je bij hen terecht. Je kan hen bereiken via een ICT-ticket of telefonisch op 75220.
- Je mag beperkt gebruik maken van ICT-middelen voor privédoeleinden op voorwaarde dat je de uitvoering van je taken en de dienstverlening van het bestuur niet in het gedrang brengt en je dit niet doet voor commerciële of mogelijk aanstootgevende doeleinden (zoals spelletjes spelen, gokken, pornografie).
- Draag bij uitdiensttreding alle provinciale ICT-middelen terug over aan jouw collega's (zoals digitale bestanden, distributielijsten, gedeelde accounts) of aan het departement ICT (zoals hardware, authenticatiemiddelen).

Gegevensopslag en informatiedeling

Als provinciale medewerker heb je toegang tot heel wat (digitale) informatie. Hou hierbij rekening met de volgende principes bij de keuze van het geschikte opslagmedium en het delen van informatie:

- Bewaar je persoonlijke, werkgerelateerde documenten in je Documenten map (die verwijst naar je H-schijf) of in je OneDrive voor Bedrijven. Deze worden regelmatig geback-upt om het gegevensverlies bij incidenten te minimaliseren.
- Persoonlijke (niet-werkgerelateerde) documenten mag je ook in beperkte mate (dus bv. niet heel je fotocollectie) op deze media bewaren in een folder genaamd 'Persoonlijk' of met de aanduiding 'Persoonlijk' in de titel van het document. Alle documenten die niet expliciet als 'Persoonlijk' worden aangeduid, worden beschouwd als werkgerelateerd.

  Ter info: In uitzonderlijke gevallen (bv. bij langdurige afwezigheid wegens ziekte), kan een leidinggevende aan ICT vragen om een collega toegang te geven tot jouw werkgerelateerde gegevens om de continuïteit van de dienstverlening te garanderen. ICT zal dit enkel doen na expliciete goedkeuring van de provinciegriffier en met de uitdrukkelijke melding dat de als 'Persoonlijk' aangeduide documenten niet mogen bekeken worden.
- Documenten die je regelmatig deelt met andere collega's bewaar je op SharePoint of de M- of N-schijf (voor documenten binnen je departement). Deze worden ook regelmatig geback-upt.
- Bewaar geen documenten op je C-schijf, je bureaublad of je downloads folder. Deze worden niet geback-upt en de gegevens kunnen dus verloren gaan bij een incident (zoals een malwarebesmetting of een crash van de pc).
- Beperk het gebruik van gratis clouddiensten, zoals Dropbox, WeTransfer, Google Forms enzovoort. Geef de voorkeur aan een platform dat ondersteund is door de provincie, zoals het Office 365 platform (met o.a. SharePoint en Microsoft Forms), aangezien deze in orde zijn qua authenticatie, beveiliging, licenties enzovoort.

- Vertrouwelijke documenten (met bijvoorbeeld persoonsgegevens) bewaar je met zorg. Je zet ze niet op een publiek toegankelijk medium, zoals een cloudopslagdienst zonder authenticatie (aanmelding) of een USB-gegevensstick. Wil je dit toch doen, sla ze dan op in versleutelde vorm, zodat de inhoud onleesbaar is bij verlies of diefstal.

  Tip: Office-documenten kan je versleutelen door ze te beveiligen met een wachtwoord. Andere soorten van documenten kan je toevoegen aan een met wachtwoord beveiligd zip-bestand. Het wachtwoord geef je via een apart kanaal door aan de ontvanger (bv. via telefoon of een aparte e-mail).

- Wees kritisch over welke informatie je deelt met derden en hoe je dit doet. Deel vertrouwelijke informatie enkel met personen die nood hebben aan deze informatie en zorg ervoor dat zij zich moeten authenticeren (door aan te melden of door een wachtwoord in te geven) vooraleer ze deze gegevens kunnen inkijken. Deel vertrouwelijke gegevens ook niet met familie of vrienden.

  Tip: Het Office 365 platform (met o.a. SharePoint, OneDrive en Teams) geeft je heel wat mogelijkheden om informatie op een veilige manier te delen. Je kan bijvoorbeeld individuele documenten delen (i.p.v. een hele bibliotheek), een verlooptijd instellen waarna het document niet meer kan geraadpleegd worden, een wachtwoord opgeven om het document te beveiligen of verhinderen dat het document wordt gedownload.

- E-mail is een (onveilig) communicatiemiddel, geen opslagmedium. Digitale informatie bewaar je en deel je best via andere platformen. Je kan e-mail wel gebruiken om een hyperlink door te sturen naar informatie op een veilig platform. Waak bij het versturen van e-mails over de distributielijst – wees dus ook zuinig met 'allen beantwoorden'.

  Tip: Het doorverwijzen naar een ander platform heeft, naast de veiligheid, als bijkomend voordeel dat de ontvanger steeds de laatste versie te zien krijgt en dat er minder netwerkbandbreedte wordt verbruikt.

- Druk informatie alleen af wanneer je ze echt nodig hebt op papier. Laat afgedrukte documenten met vertrouwelijke informatie niet liggen bij de printer of rondslingeren op je bureau.

Toegangsbeveiliging

Als provinciale medewerker beschik je over een aantal aanmeldingsgegevens – gebruikersnaam en wachtwoord – om toegang te verkrijgen tot ICT-middelen. Hou bij het gebruik hiervan rekening met de volgende richtlijnen:

- Je aanmeldingsgegevens zijn persoonlijk. Je deelt ze dus niet met collega's, familie of kennissen en je schrijft ze nergens op. Je meldt je ook nooit aan met de aanmeldingsgegevens van een collega. Je bent immers persoonlijk aansprakelijk voor alle handelingen die met jouw aanmeldingsgegevens worden uitgevoerd.

- Stel elke 6 maanden een uniek, sterk wachtwoord in voor al je provinciale gebruikersaccounts. Kies m.a.w. een wachtwoord dat:

  - verschilt van al je andere (en vorige) wachtwoorden, en zeker van je wachtwoorden voor persoonlijk (niet-professioneel) gebruik;
  - bestaat uit minimaal 8 tekens uit 3 van de 4 tekengroepen (hoofdletters, kleine letters, cijfers en andere tekens);
  - niet gemakkelijk te raden is (bv. gebaseerd op jouw naam of jouw kinderen, opeenvolgende cijfers of letters).

  Tip: Suggesties voor een sterk wachtwoord (of een wachtwoordzin) – en voor het gebruik van een wachtwoordkluis – kun je vinden op SafeOnWeb.

- Heb je een vermoeden dat je wachtwoord niet meer vertrouwelijk is? Wijzig dat dan zo snel mogelijk.
- Als je een account hebt aangevraagd voor gedeeld gebruik (bv. een account voor een leverancier), dan ben je verantwoordelijk voor het wachtwoordbeheer hiervan. Wijzig dus het wachtwoord als één van de gebruikers van de account hem niet meer nodig heeft. Zorg er ook voor dat de gebruikers van de account gebonden zijn aan de arbeidsvoorwaarden van de provincie (o.a. deze dienstnota) (bv. door dit te vermelden in een stagecontract of een aparte integriteitsverklaring op te maken).
- Beveilig ook persoonlijke toestellen, zoals een persoonlijke smartphone of thuis-PC, met een wachtwoord of pincode als er provinciale informatie, zoals e-mails, op staat.
- Vergrendel jouw PC als je je bureau verlaat – ook bij korte afwezigheden.

  Tip: Je kunt dit doen door op de Windows toets en L te drukken. Op Ctrl, Alt en Delete drukken en vervolgens 'Deze computer vergrendelen' selecteren werkt ook.

E-mail en internet

Als provinciale medewerker maak je gebruik van e-mail en het internet om je taken uit te voeren. Hou hierbij rekening met de volgende richtlijnen:

- Wees waakzaam voor verdachte e-mailberichten. Deze herken je aan één of meerdere van de volgende kenmerken:
  - verstuurd in naam van iemand of een instantie die je kent of vertrouwd overkomt;
  - verstuurd vanuit een vals e-mailadres;

    Tip: Kijk hierbij vooral naar het domein van het e-mailadres. Dit zijn de 2 laatste 'woorden' achter de '@' (bv. bij 'info@provincie.antwerpen.be' is dit 'antwerpen.be', m.a.w. het domein van de stad antwerpen, terwijl dit voor de provincie 'provincieantwerpen.be' moet zijn).

    Let op: Dit is niet altijd het geval, want een e-mailadres kan nagebootst worden of de mailbox kan gehackt zijn.
  - niet aan jou persoonlijk gericht, maar beginnend met een onpersoonlijke aanhef (bv. 'beste' of 'geachte klant');
  - onverwachte boodschap met dwingend karakter (bv. 'je wint een prijs als …' of 'je krijgt een boete tenzij je reageert binnen de 24 uur');

  - hyperlink naar een kwaadaardige website (phishing of malware);

    Tip: Kijk hierbij vooral naar het domein van het e-mailadres. Dit zijn de 2 laatste 'woorden' vóór de eerste schuine streep (/), waarbij een punt (.) de scheiding vormt tussen de woorden (bv. bij 'www.provinc.ie/antwerpen.be' is dit 'provinc.ie', m.a.w. een domein uit Ierland (landcode IE)).

    Let op: kijk hiervoor niet naar de tekst van de hyperlink maar 'zweef' met de muiscursor boven de link om te zien waarnaar de link verwijst.
  - taal- en stijlfouten.
- Wees waakzaam voor verdachte websites. Deze herken je aan één of meerdere van de volgende kenmerken:
  - verdachte URL (webadres);

    Tip: Kijk hierbij vooral naar het domein van de website. Dit zijn de 2 laatste 'woorden' achter het apenstaartje (@), waarbij een punt (.) de scheiding vormt tussen de woorden (bv. bij 'info@provincie.antwerpen.be' is dit 'antwerpen.be').
  - waarschuwing van je webbrowser dat de website onveilig is (bv. omdat er geen gebruik wordt gemaakt van https);
  - formulier waarin je gevraagd wordt om aan te melden met je (provinciale) gebruikersaccount of om bepaalde (vertrouwelijke) gegevens door te geven (bv. informatie over de werking van de provincie, financiële gegevens);
  - automatische installatie van software of de vraag om dit handmatig te doen.

  Tip: Gebruik de website VirusTotal.com om een verdachte URL te controleren. Deze website controleert de door jou ingegeven URL aan de hand van een 70-tal antivirusscanners.
- Reageer niet op verdachte e-mailberichten: open geen bijlagen en klik niet op de hyperlinks in het bericht. Stuur ze door naar verdacht@provincieantwerpen.be, zodat de ICT-collega's de spamfilter kunnen bijsturen indien nodig, en verwijder ze nadien. Bij twijfel contacteer je de afzender (bv. telefonisch) of de ICT-servicedesk.

  Tip: Vertrouw je de afzender? Meld je dan af voor toekomstige berichten. Meestal vind je hiervoor een uitschrijflink onderaan het bericht. Klik hier nooit op als je de afzender niet vertrouwt, want zo bevestig je aan de afzender dat je e-mailadres in gebruik is en zal je voortaan mogelijk nog meer ongewenste berichten krijgen.
- Geef jouw provinciaal e-mailadres niet door aan derden (of aan websites) tenzij dit werkgerelateerd is. De kans is dan immers groter dat je e-mailadres in verkeerde handen terechtkomt (bv. doordat hackers voortdurend proberen om websites te hacken) waardoor je meer spam en andere ongewenste e-mail zult ontvangen.
- Als je vermoedt dat je toestel is besmet met malware, schakel het dan onmiddellijk uit of verbreek de netwerkverbinding (door de netwerkkabel uit te trekken of de Wi-Fi-verbinding uit te schakelen). Contacteer vervolgens de ICT-servicedesk.

- Je mag je provinciale e-mail ook in beperkte mate gebruiken voor persoonlijke doeleinden. Bewaar dergelijke e-mails in een folder genaamd 'Persoonlijk' of gebruik deze aanduiding in de titel van je e-mail. Alle e-mails die niet expliciet als 'Persoonlijk' worden aangeduid, worden beschouwd als werkgerelateerd.

  Ter info: In uitzonderlijke gevallen (bv. bij langdurige afwezigheid wegens ziekte), kan een leidinggevende aan ICT vragen om een collega toegang te geven tot jouw werkgerelateerde gegevens om de continuïteit van de dienstverlening te garanderen. ICT zal dit enkel doen na expliciete goedkeuring van de provinciegriffier en met de uitdrukkelijke melding dat de als 'Persoonlijk' aangeduide e-mails niet mogen bekeken worden.

Software

Als provinciale medewerker krijg je een PC ter beschikking met vooraf geïnstalleerde software (zoals het Office-pakket en een webbrowser) en krijg je toegang tot enkele web-gebaseerde toepassingen (zoals het Office 365-platform en het systeem voor tijdsregistratie). Je kan echter zelf ook software installeren op je PC en je kan ook zelf gebruik maken van (al dan niet gratis) cloud toepassingen. Hou hierbij rekening met de volgende richtlijnen:

- Ga na of het departement ICT geen software aanbiedt met de gevraagde functionaliteit. Dan is er immers automatisch voldaan aan de volgende richtlijnen. Je maakt hiervoor een ICT-ticket aan.
- Zorg dat je de nodige licenties hebt om de software te mogen gebruiken.

  Let op: Vele 'gratis' tools zijn gratis voor persoonlijk gebruik, maar niet voor professioneel gebruik. Lees daarom goed de licentievoorwaarden.
- Ga na of de software die je wilt gebruiken veilig is.

  Let op: 'Gratis' tools bevatten vaak malware (computervirussen), gaande van relatief onschuldige adware, waarmee je advertenties voorgeschoteld krijgt, tot meer kwaadaardige vormen die je PC beschadigen of informatie stelen.

  Tip: Gebruik de website VirusTotal.com om een installatiebestand of website te controleren op malware.
- Hou software die je zelf installeert up-to-date. Installeer m.a.w. altijd de meest recente (veiligheids)updates en herstart je toestel nadien als je daarom gevraagd wordt. (Dit laatste geldt ook voor de software updates die het departement ICT uitvoert op jouw toestel.)
- Verwerkt de software die je wilt gebruiken persoonsgegevens? Breng dan je DPO op de hoogte, zodat de nodige maatregelen kunnen getroffen worden in het kader van de GDPR.

Hardware

- Breng zelf geen fysieke wijzigingen of uitbreidingen aan de provinciale hardware of het provinciale netwerk aan. Installeer bijvoorbeeld zelf geen (Wi-Fi)routers, switches of hubs om het netwerk uit te breiden.
- Verplaats geen toestellen die een vaste locatie hebben zonder toestemming van de ICT-collega's.
- Leen geen provinciale hardware uit aan derden, tenzij toegestaan door je leidinggevende.

Mobiele toestellen en telewerken

Als provinciale medewerker krijg je een aantal mobiele toestellen (bv. laptop, tablet, smartphone) en andere hardware (bv. printers, ICT-netwerk) ter beschikking om je taken uit te voeren. Hou hierbij rekening met het volgende:

- Neem je jouw mobiel toestel mee naar huis? Laat hem dan niet onbeheerd achter (bv. in de wagen).
- Gebruik bij voorkeur je provinciale laptop om te telewerken. Op dit toestel werden immers de nodige tools voorzien om op een gebruiksvriendelijke en veilige manier te verbinden met het provinciale netwerk en de provinciale toepassingen.

  Let op: Om verbinding te kunnen maken met het provinciale netwerk via vpn, moet je toestel een up-to-date besturingssysteem (Windows) en antivirustoepassing hebben.

  Let op: Als je werkt op een gedeelde pc, meld dan na gebruik af van alle toepassingen en websites en sla geen wachtwoorden op in de webbrowser.
- Volg de richtlijnen uit de dienstnota 'Mobiel bellen en internet (DICT-2)', in het bijzonder de afspraken rond beschadiging, defect, diefstal en verlies van je toestel.
- Bij verlies of diefstal van een persoonlijk toestel met bedrijfsgegevens (zoals e-mail), laat je dit ook weten aan de ICT-servicedesk. Zo kunnen ze proberen om de bedrijfsgegevens op dit toestel vanop afstand te blokkeren of te wissen.

  Tip: De ICT-servicedesk kan, indien gewenst, proberen om het volledige toestel (inclusief persoonlijk gegevens) te wissen. Ze doen dit enkel na een expliciete vraag van jou.
- Maak zoveel mogelijk gebruik van beveiligde Wi-Fi-verbindingen of van het mobiel data netwerk. Bij onbeveiligde Wi-Fi-netwerken zijn je gegevens leesbaar op het netwerk. Vooral op publieke plaatsen (station, restaurant, winkel) loop je het risico dat iemand je afluistert.
- Wees waakzaam als je werkt aan vertrouwelijke dossiers in een openbare ruimte: zorg dat je scherm niet kan afgelezen worden, laat geen papieren documenten rondslingeren, hou geen vertrouwelijke gesprekken, leg je toestel vast met een beveiligingskabel en vergrendel het als je je bureau verlaat.

Toezicht en handhaving

Je leidinggevenden, de DPO en het departement ICT hebben, rekening houdend met de privacywetgeving, het recht om te controleren of je de bepalingen van deze dienstnota naleeft.

Voor de controle op het gebruik van internet en e-mail is er een specifieke procedure uitgewerkt in het arbeidsreglement.

Maarten Ronny Puls
De Provinciegriffier

23/06/2022