GGD
Gooi en Vechtstreek

Richtlijnen voor veilig thuiswerken (versie 2.0)

De Regio blijft doorwerken tijdens de coronacrisis. Wie dat kan, doet dat thuis. Maar let op: voor cybercriminelen is deze crisis een kans om gevoelige data buit te maken. En een foutje is snel gemaakt, waardoor gevoelige gegevens op straat kunnen komen te liggen. Volg onderstaande richtlijnen en voorkom dat er gegevens over inwoners of collega's in verkeerde handen vallen.

Door het naleven van deze regels kunnen we zo zorgvuldig en zo veilig mogelijk thuis werken met middelen die door de Regio beschikbaar zijn gesteld (smartphone, laptop) of met eigen apparatuur.

1. Werk bij voorkeur met de middelen die door de Regio beschikbaar zijn gesteld, zoals iPhone, iPad en laptop;
2. Indien eigen apparatuur wordt gebruikt (computer, laptop, privételefoon), dan mag op de schijven hiervan geen bedrijfsinformatie en gevoelige (persoons)informatie worden opgeslagen;
3. Werk voor wat betreft vak-applicaties zoveel mogelijk binnen de beveiligde werkomgeving via Ericom Blaze. Kun je in je werk volstaan met enkel de mail dan is het dringend verzoek om dat zoveel mogelijk via webmail te doen;
4. Gebruik altijd je werkmailadres en werktelefoonnummer (indien beschikbaar) voor zakelijke communicatie;
5. Wees voorzichtig met het gebruik van (video)chatdiensten. Bellen en SMS is nog steeds het makkelijkst en veiligst. Over de mogelijkheden om online te vergaderen (waaronder videobellen) is al eerder een stappenplan gecommuniceerd waarin eerst naar de veiligste opties moet worden gekeken en pas in laatste instantie naar de minst veilige opties.
6. Bewaar het gebruikerswachtwoord om in je je laptop te komen niet op een briefje op of in de laptop maar leer het uit je hoofd;
7. Sla geen documenten lokaal op je laptop op, zeker niet als je huisgenoten van dezelfde laptop gebruik maken. Andersom: bescherm jezelf en je huisgenoten tegen het uitlekken van persoonlijke documenten als de laptop weer terug moet naar ICT.
8. Ga zorgvuldig om met mobiele apparatuur: niet onbeheerd achterlaten in bijvoorbeeld een vervoermiddel of een ruimte waarin andere personen aanwezig zijn;
9. Indien de werkplek wordt verlaten en er andere mensen in de woning aanwezig zijn, dien je Ericom Blaze (tijdelijk) af te sluiten;
10. Gegevens die je verwerkt namens de Regio zijn vertrouwelijk, dus niemand kijkt mee/luistert mee. Wees net als altijd extra voorzichtig met bijzondere persoonsgegevens, zoals medische gegevens;
11. Laat eventueel in bezit zijnde fysieke documenten van de Regio niet onbeheerd en berg ze goed op. Wil je ze vernietigen, neem ze dan t.z.t. weer mee naar de Regio en gooi ze in de daarvoor bestemde zilveren papiercontainers;
12. Neem geen fysieke documenten/dossiers met persoonsgegevens mee naar huis, tenzij het praktisch echt niet uitvoerbaar is om dit op een andere manier te doen, bijvoorbeeld door te digitaliseren/scannen. Desnoods maak je gebruik van een versleutelde USB-stick (te verkrijgen bij de ICT servicedesk);
13. Let op phishingmails/sms-jes. Dit zijn berichten die door kwaadwillenden aan mensen worden gestuurd om hen aan de hand van een actueel thema (zoals nu corona) te verleiden persoonlijke gegevens te verstrekken. Krijg je berichten die je niet verwacht of die van een onbekende afzender zijn? Klik dan niet op links in deze berichten, open geen bijlagen en vul geen gegevens in. Zie hierover ook dit eerdere bericht op de Binnenband;
14. Wees voorzichtig met het gebruik van cloud- of opslagdiensten, zeker wanneer deze gratis zijn. Want het zou kunnen dat zo'n dienst juist gratis is omdat de aanbieder je gegevens gebruikt voor andere doeleinden of omdat geen aandacht is besteed aan beveiliging.
15. Zorg dat je altijd goed bereikbaar bent voor je collega's (en externen/derden) voor vragen en overleg.
16. Probeer te voorkomen dat een datalek ontstaat met deze tips.
17. Neem je verantwoordelijkheid voor informatiebeveiliging als er toch iets fout gaat of als je verdachte zaken ziet en meld dit direct bij de ICT Service Desk (via (035) 692 62 00 of meldpuntdatalek@regiogv.nl) of maak een melding via de Binnenband.

[redacted]

4 maart 2021

Melden datalekken

Wat is een datalek?
We spreken van een datalek als sprake is van toegang tót of vernietiging, wijziging of vrij komen ván persoonsgegevens zonder dat dit de bedoeling is. Ook als redelijkerwijs niet kan worden uitgesloten dat dit gebeurd is, is sprake van een datalek. Een persoonsgegeven betreft informatie die direct over iemand gaat óf naar deze persoon te herleiden is. Voorbeelden van persoonsgegevens zijn het burgerservicenummer, naam, adres en geboortedatum, maar ook medische informatie en geloofsovertuiging. Meest in het oog springend zijn datalekken naar derden buiten onze organisatie. Maar ook tussen collega's onderling kan sprake zijn van lekken. Denk hierbij aan de onbedoelde inzage in iemands personeelsdossier door een onbevoegde. Datalekken ontstaan (ook bij de Regio) in de meeste gevallen door handelen van medewerkers en niet door onvoldoende technische beveiliging. Meest voorkomend zijn de gevallen waarin derden die geen toegang tot die gegevens mogen hebben, toch toegang hebben gekregen. Vaak gaat het om digitale bestanden die per ongeluk beschikbaar zijn of zijn toegestuurd aan onbevoegden. Maar een verloren of gestolen geprint dossier is evengoed een datalek.

Voorbeelden van mogelijke datalekken zijn:

- kwijtraken van een brief met persoonsgegevens bij de post
- verzenden van persoonsgegevens naar een verkeerd e-mailadres
- versturen van te veel (onnodige) gegevens aan derden
- kwijtraken van een onbeveiligde USB-stick met persoonsgegevens
- diefstal van een laptop, iPad e.d. met persoonsgegevens
- een malware besmetting

Tips voor voorkomen datalekken:

- Laat je spullen niet onbeheerd op je bureau achter.
- Laat je laptop niet in de auto achter.
- Lock je computer met 'Windows vlaggetje L' als je je werkplek verlaat
- Bewaar persoonsgegevens niet langer dan nodig. Wat je niet hebt, kun je ook niet lekken. Verwijder de databestanden die je niet meer nodig hebt. Denk hierbij ook aan papieren documenten, gooi deze weg in de papierkliko op het werk en níet thuis bij het oud papier.
- Deel alleen gegevens die voor de ontvanger noodzakelijk zijn om het werk uit te voeren. Denk er bij het versturen van Excel documenten aan dat je alleen de relevante kolommen/werkbladen meestuurt.
- Controleer vóór het versturen nog even het opgestelde mailtje:
  o Kloppen de geadresseerden?
  o Heb je de juiste bijlage bijgevoegd?
  o Is het gevoelige informatie die je naar buiten de organisatie verstuurt? In dat geval gebruik je Zivver.
- Wees alert bij de printer:
  o papier op? Loop dan niet weg maar vul direct het papier bij, anders komt je opdracht er mogelijk bij een ander uit.
  o storing tijdens het printen? Geef dan aan ICT Servicedesk door dat de printopdracht gevoelige gegevens bevat.

Wat te doen bij een datalek?

- Merk je dat er mogelijk sprake is van een datalek dan moet je dit direct melden bij ICT Servicedesk. Dat kan telefonisch: **(035) 692 62 00**, via meldpuntdatalek@regiogv.nl of gebruik het formulier hieronder. De collega's van ICT ondernemen dan actie.
  Vervolgens beoordeelt het Team Privacyincidenten (nieuwe naam!) of het daadwerkelijk een datalek is en of het datalek extern gemeld moet worden bij de toezichthouder, de Autoriteit Persoonsgegevens, en eventueel ook bij degene wiens gegevens het betreft. Dit is het geval als er een (hoog) risico voor personen is.

Het is niet erg om een datalek intern te melden. De organisatie wordt er vaak scherper van. Bij twijfel schroom niet en meld het mogelijke datalek! De handreiking 'Beoordeling datalekken AVG en 'Memo Interne procedure afhandeling meldingen datalekken AVG' staan op de Binnenband of zijn op te vragen bij [redacted] (corona@ggdgv.nl)

Tips ter voorkoming van datalekken

Een datalek ontstaat gemakkelijk bij onachtzaamheid. Hier vind je tips om dat te voorkomen.

In het algemeen
De onderstaande tips vinden vooral hun oorsprong in onze Bruikleenovereenkomst. Het is hoe dan ook verstandig deze nog eens door te lezen en je te houden aan de daarin gestelde richtlijnen.

Zakelijke apparatuur in bruikleen?
Het spreekt voor zich dat je zorgvuldig omgaat met apparatuur die door de werkgever aan jou in bruikleen is gegeven. Beschadiging en verlies/diefstal die jou is aan te rekenen, zijn voor eigen rekening.

Gebruik je een iPad, iPhone of andere Smartphone?
Zorg ervoor dat het apparaat met een pincode is beveiligd. Bij nieuwere typen van dergelijke apparaten kan ook een vingerafdruk of gezichtsherkenning worden ingesteld. Maak ook op je privé-smartphone gebruik van dergelijke beveiligingsmiddelen, zeker als je daarop ook je zakelijke e-mail synchroniseert.

iPad of iPhone verloren of gestolen?
Een verloren of gestolen iPad of iPhone kan op afstand worden gewist zodra het apparaat verbinding maakt met Internet. Team ICT kan dat voor je verzorgen maar nog beter is het om dat zelf te doen zodat er minder tijd verloren gaat. Op het Serviceplein bij Handleidingen staat hoe je dat moet doen.

Gebruik je USB-sticks?
Gebruik geen USB-sticks die privé eigendom zijn. Mocht het nodig zijn om op deze manier zakelijke bestanden te vervoeren, gebruik dan een beveiligde stick. Deze is via het Serviceplein aan te vragen en bevat een beveiligde zone waarin je zakelijke bestanden kunt plaatsen. Een USB-stick raak je gemakkelijk kwijt (in een pc laten zitten, vergeten mee te nemen of verloren), vandaar dat extra oplettendheid hierbij geboden is.

Privacy?
Op zakelijke laptops mogen natuurlijk geen privacy-gevoelige gegevens achterblijven. Dit geldt ook voor de leenlaptops die je via het Serviceplein voor korte tijd kunt reserveren. Mocht het voor het werk toch noodzakelijk zijn om bestanden lokaal op te slaan, gebruik dan de speciaal voor dat doel ingerichte beveiligde zone. Daar kun je alleen bij als je het juiste wachtwoord kent. Verwijder na gebruik alle gegevens die je op de laptop hebt opgeslagen uit de mappen 'Mijn documenten', 'Downloads' en van het bureaublad etc.

Deel je privacygevoelige gegevens?
Maak geen gebruik van onveilige websites zoals Dropbox, WeTransfer of Google Cloud om privacygevoelige gegevens met externe partijen te delen. Gebruik hiervoor het NAS systeem waarmee je zowel kunt verzenden als ontvangen. Meer informatie hierover is aan te vragen bij de ICT Servicedesk. Op niet al te lange termijn wordt de software Zivver bedrijfsbreed geïmplementeerd waarmee veilig mailen en meesturen van grote bestanden mogelijk is. Houd de berichtgeving hierover in de gaten).

Installeren van software
Op in bruikleen gegeven apparatuur mag uiteraard geen software worden toegevoegd. Ontbreekt benodigde software, dan neem je contact op met ICT.

Pas op met e-mail
Zowel zakelijk als privé: open geen e-mail waarvan je de herkomst niet kent en klik niet op linkjes of onbekende bijlagen. Het is niet logisch dat je e-mails van bijvoorbeeld banken of internetproviders op je zakelijk mailadres ontvangt; die bevatten meestal ransomware, virussen of pogingen tot phishing. Het bekende TV-programma 'Opgelicht' heeft een goede gratis app met dezelfde naam gemaakt die hierbij behulpzaam is. Je ontvangt dan waarschuwingen voor valse mail of websites die tot doel hebben jou inloggegevens te ontfutselen. Tenslotte: gebruik je zakelijke e-mail adres niet voor privé doeleinden zoals inloggen bij webwinkels of het ontvangen van vakantie-aanbiedingen.