Veiligheidsregio Rotterdam-Rijnmond

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 768

25 juli 2023

Officiële uitgave van de gemeenschappelijke regeling Veiligheidsregio Rotterdam-Rijnmond

Regeling ICT- en informatiegebruik VRR 2023

Het Dagelijks Bestuur van de Veiligheidsregio Rotterdam-Rijnmond,

Overwegende dat:
- de Regeling ICT- en informatiegebruik 2012 zoals die gold op 31 december 2019 in de gemeente Rotterdam door de Veiligheidsregio integraal is overgenomen
- de Regeling ICT- en informatiegebruik 2012 verouderd is en op diverse punten aanpassing behoeft;

gelet op:
- artikel 125, artikel 125ter Ambtenarenwet in samenhang met artikel 11.2 Aanpassingswet WNRA;
- artikel 33b, eerste lid, onder c van de Wet gemeenschappelijke regelingen;
- het positieve advies van de Centrale ondernemingsraad van 10 mei 2023;

besluit vast te stellen:

Regeling ICT- en informatiegebruik VRR 2023

Artikel 1 Begripsbepalingen

1. De begripsbepalingen van artikel 4 van de AVG zijn van overeenkomstige toepassing op deze regeling.
2. In afwijking van artikel 4, onderdeel 19, van de AVG wordt onder concern verstaan: het geheel aan directies binnen de VRR en de overige daaronder vallende afdelingen.
3. In deze regeling wordt verstaan onder:
   - a AVG: Verordening (EU) 2016/679 van het Europees parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met verwerking van persoons- gegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming);
   - b beveiligingsincident: gebeurtenis die een bedreiging vormt of kan vormen voor de vertrouwelijkheid, integriteit of beschikbaarheid van gegevens;
   - c beveiligingsclassificatie: inschaling van de risicoklasse van (informatie in) processen;
   - d CIO: Chief Information Officer;
   - e CISO: Chief Information Security Officer
   - f datalek: inbreuk in verband met de persoonsgegevens als bedoeld in artikel 1, onderdeel 12, van de AVG;
   - g elektronische informatie- en communicatiefaciliteiten: sociale media, e-mail-, internet- en telefoonfaciliteiten, Whatsapp, SMS en alle vergelijkbare communicatie toepassingen;
   - h FG: functionaris gegevensbescherming als bedoeld in afdeling 4 van de AVG;
   - i ICT-apparatuur: elektronische informatie- en communicatiemiddelen inclusief alle bijbehorende hard- en software en bestanden die door of namens de VRR aan medewerkers beschikbaar is gesteld;
   - j ICT-middelen: alle elektronische informatie- en communicatiefaciliteiten en ICT-apparatuur waar VRR-informatie mee verwerkt wordt, alsmede de privé ICT-middelen voor zover zij gebruikt worden voor de uitvoering van de door of namens de VRR opgedragen taken;
   - k IRT: Incident Response Team, bestaande uit de CIO, CISO, het Hoofd ICT, het Hoofd IM en de FG;
   - l medewerker: ambtenaar in de zin van het Ambtenarenreglement, dan wel degene die op basis van de Cao Ambulancezorg werkzaamheden verricht voor en/of bij de VRR, dan wel degene die betaalde of niet betaalde werkzaamheden voor (een onderdeel van) de VRR verricht;
   - m onrechtmatig gebruik dan wel misbruik van de ICT-middelen en VRR-informatie: doen of nalaten in strijd met deze regeling of andere wet- en regelgeving;
   - n privébestand: bestand met een geheel of overwegend persoonlijke inhoud;
   - o privé ICT-middelen: ICT-apparatuur in eigendom van medewerker zelf of anderszins verkregen, zonder dat deze door de VRR beschikbaar is gesteld;
   - p VRR-informatie: alle VRR-informatie waaronder begrepen informatie verwerkt met elektronische informatie- en communicatiefaciliteiten en informatie van ketenpartners, niet zijnde openbare VRR-informatie;
   - q zakelijk gebruik: het verwerken van VRR-informatie voor de uitvoering van de door de VRR opgedragen taken.

Artikel 2 Gebruik van ICT-middelen en VRR-informatie

1. Medewerkers gebruiken de ICT-middelen en VRR-informatie primair en hoofdzakelijk voor het uitvoeren van hun werkzaamheden in overeenstemming met regelgeving en het doel waarvoor de middelen en informatie zijn verstrekt.
2. Het is medewerkers verboden om ICT-middelen aan een ander ter beschikking te stellen. VRR-informatie mag slechts verstrekt worden aan daartoe geautoriseerde anderen.
3. De ICT-middelen en VRR-informatie worden beschikbaar gesteld voor zakelijk gebruik. Privégebruik van VRR-informatie, niet zijnde openbare informatie, is niet toegestaan.
4. Gepast privégebruik door de medewerkers van door de VRR ter beschikking gestelde apparaten (ICT-apparatuur) is toegestaan, mits dit gebruik in overeenstemming is met deze regeling en dit gebruik niet ten koste gaat van het uitvoeren van de werkzaamheden. Misbruik, dat wil zeggen overmatig, uitbundig, storend of schadelijk privégebruik, is niet toegestaan.
5. Gebruik van de ICT-middelen of VRR-informatie voor commerciële doeleinden is niet toegestaan.
6. Mits de medewerker zich houdt aan deze regeling, mag de medewerker gebruikmaken van privé ICT-middelen voor het benaderen van informatie van de VRR voor het uitvoeren van werkzaamheden.
7. De medewerker is verantwoordelijk voor het beschikbaar stellen en binnen de VRR-omgeving bewaren van VRR-informatie.
8. Het is medewerkers niet toegestaan om ICT-middelen van de VRR te gebruiken:
   a voor het opvragen, versturen, vastleggen of anderszins verwerken van pornografisch, erotisch, dan wel racistisch materiaal;
   b voor het opvragen, versturen, vastleggen of anderszins verwerken van informatie die naar algemeen maatschappelijke opvattingen als lasterlijk, beledigend, aanstootgevend of oneervol wordt beschouwd;
   c om online te gokken;
   d om software, films of muziek te downloaden;
   e voor het doorsturen van ongecontroleerde informatie naar cloudoplossingen of privé-opslag thuis; of
   f voor het afnemen van een dienst waarvan de kosten ten laste komen van de VRR.
9. Het verbod, bedoeld in het vorige lid, geldt niet indien het gebruik nodig is voor de vervulling van de taak en hierover overleg heeft plaatsgevonden met de leidinggevende.
10. Het is medewerkers niet toegestaan om zonder toestemming van hun leidinggevende bij het gebruik van de ICT-middelen een belasting van de ICT-omgeving te creëren waarvan de medewerker redelijkerwijs moet begrijpen dat deze de ICT-dienstverlening negatief beïnvloedt. Hieronder wordt in ieder geval gerekend:
    a het versturen van een mail waarvan de groep tegelijkertijd geadresseerden te omvangrijk is;
    b het geautomatiseerd doorsturen van mail naar een extern e-mailadres.
11 Zodra een medewerker door een ICT-medewerker wordt gewezen op een door zijn toedoen te hoge belasting van de ICT-omgeving, beëindigt de medewerker deze activiteiten onmiddellijk, tenzij hij handelt met toestemming van zijn leidinggevende.
12 Medewerkers betrachten bij het gebruik van de ICT-middelen en VRR-informatie de nodige zorgvuldigheid en waarborgen de integriteit en goede naam van de VRR.
13 Medewerkers handelen volgens de gestelde beveiligingseisen overeenkomstig het privacy- en informatiebeveiligingsbeleid ten aanzien van ICT-middelen en VRR-informatie.
14 De medewerker heeft een eigen verantwoordelijkheid over het juiste gebruik van ICT-middelen en om de kosten van het gebruik van de ICT-middelen zoveel mogelijk te beperken.
15 Zakelijk gebruik van ICT-middelen of VRR-informatie in het buitenland is toegestaan, tenzij er sprake is van gebruik in een land met een hoog risico op digitale spionage of cybercriminaliteit. De medewerker die ICT-middelen van de VRR of VRR-informatie buiten de Europese Unie gebruikt, informeert vooraf bij de Servicedesk indien het land waarin het gebruik zal plaatsvinden een hoog risico op digitale spionage of cybercriminaliteit heeft. Indien dat het geval is, handelt de medewerker in overeenstemming met het advies van de Servicedesk.
16 Medewerkers melden schade aan en verlies of diefstal van ICT-middelen of VRR-informatie direct bij de Servicedesk en leidinggevende.

Artikel 3 Toegang tot en beveiliging van VRR-informatie

1. De medewerker verschaft zich uitsluitend toegang tot die informatie waartoe hij geautoriseerd is.

2. Ingeval van wijziging van de functie van de medewerker meldt de leidinggevende direct aan de Servicedesk de niet langer noodzakelijke autorisaties en levert de medewerker de niet-noodzakelijke ICT-middelen in.
3. Het is de medewerker verboden om anderen dan daartoe geautoriseerde medewerkers toegang tot VRR-informatie te verlenen, behoudens met toestemming van zijn leidinggevende. Deze toegang vindt niet plaats als de aard van de informatie zich daarvoor niet leent.
4. De medewerker neemt passende technische en organisatorische maatregelen om VRR-informatie te beveiligen tegen verlies of tegen enige vorm van onrechtmatig gebruik. De medewerker houdt hierbij in ieder geval rekening met:
   a de mate van vertrouwelijkheid van de informatie;
   b de door de VRR gestelde beveiligingsvoorschriften en het privacy- en informatiebeveiligingsbeleid van de VRR. Het informatiebeveiligingsbeleid omvat een kader met regels voor het beschermen van VRR-informatie.
   c aan de werkplek verbonden risico's; en
   d het risico door het benaderen van VRR-informatie met andere dan door de VRR verstrekte ICT-apparatuur.

5. Bij gebruik van een privé ICT-middel verstrekt de medewerker op verzoek van of namens de algemeen directeur de VRR-informatie, indien deze nodig is in het kader van de uitvoering van wettelijke verplichtingen.
6. De medewerker meldt geconstateerde of vermoede beveiligingsincidenten direct bij de Servicedesk, conform de regels die hieromtrent zijn of worden opgesteld.
7. Ingeval van dringende redenen kan de algemeen directeur, dan wel de CIO of het Hoofd ICT, besluiten tot het blokkeren van een account en tot het nemen van noodmaatregelen voor de informatiebeveiliging. Deze noodmaatregelen kunnen, voor zover dit noodzakelijk is, betrekking hebben op privé-middelen en privébestanden.
8. Het Hoofd ICT is gerechtigd een account te laten blokkeren bij uitdiensttreding van de betreffende medewerker.
9. De medewerker is verplicht advies of ondersteuning van de leidinggevende te vragen indien de medewerker onvoldoende in staat is de beveiligingsvoorschriften uit te voeren of te beoordelen.
10. De medewerker kan de beveiligingsclassificatie en de beveiligingsvoorschriften opvragen bij zijn leidinggevende of bij het Hoofd IM.
11 Indien bij een door de medewerker gemeld beveiligingsincident aanwijzingen zijn dat sprake is of kan zijn van een datalek, onderzoekt het IRT samen met de medewerker en zijn leidinggevende of een datalek kan worden vastgesteld.

Artikel 4 Controle en algemene bepalingen

1. Controle op het gebruik van de ICT-middelen en VRR-informatie vindt slechts plaats door of in opdracht van de algemeen directeur, die voorafgaand hieraan het doel van de controle duidelijk omschrijft.
2. Controle vindt slechts plaats in het kader van de in artikel 7, eerste lid, genoemde doeleinden. Deze doeleinden stellen beperkingen aan de omvang en wijze van controle. Bij controle wordt het onderstaande in acht genomen:
   a controle ter verkrijging van inzicht in de mate van gebruik van de ICT-middelen en VRR-informatie wordt, behoudens een andersluidende wettelijke verplichting, beperkt tot de verkeersgegevens die betrekking hebben op tijd, hoeveelheid, omvang en dergelijke;
   b controle ter voorkoming van onrechtmatig gebruik dan wel van misbruik van de ICT-middelen en VRR-informatie wordt zo beperkt mogelijk gehouden, in die zin dat deze in redelijke verhouding staat tot het doel waarvoor deze wordt aangewend;
   c de controle vindt in beginsel geanonimiseerd en slechts steekproefsgewijs plaats;
   d voor zover de controle autorisatie of authenticatie betreft, kan de controle autorisatiegegevens betreffen;
   e controle in het kader van integriteitschendingen of het overtreden van de bepalingen uit deze regeling wordt zo beperkt mogelijk gehouden en kan slechts indien daartoe zwaarwegende redenen bestaan persoonsgegevens of de inhoud van bestanden of berichtenverkeer betreffen;
   f controle in het kader van het beheer van de toegang tot de systemen en het beveiligen van het systeem en het netwerk voor het tegengaan van virussen en andere schadelijke programma's vindt zoveel mogelijk op geautomatiseerde wijze plaats.

3. Controle vindt als regel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot individuele personen.
4. Onrechtmatig gebruik dan wel misbruik van de ICT-middelen en VRR-informatie wordt zo veel mogelijk softwarematig onmogelijk gemaakt.

5. Controle beperkt zich tot autorisatie- en verkeersgegevens van het gebruik van de ICT-middelen of VRR-informatie, tenzij noodzakelijk is een gerichte controle als bedoeld in artikel 5, uit te voeren.
6. De medewerker, die voor de uitvoering van de door de VRR opgedragen taken gebruik maakt van privé ICT-middelen, is verplicht mee te werken aan eventuele controles.
7. Indien geconstateerd wordt dat de medewerker zich niet houdt aan deze regeling, spreekt diens leidinggevende hem hier zo spoedig mogelijk op aan.
8. Het gebruik van de ICT-middelen en VRR-informatie door leden van de ondernemingsraden, Centrale Ondernemingsraad, Georganiseerd Overleg en andere medewerkers met een vertrouwensfunctie, is in beginsel uitgesloten van controle. Dit geldt niet voor de controle op de veiligheid van het elektronische verkeer en voor informatie die geen verband houdt met genoemde functies of lidmaatschappen.
9. De in het eerste lid onder b genoemde controle kan geautomatiseerd, via in het systeem ingebouwde mechanismen, plaatsvinden bij zwaarwegende redenen vanwege de aard van het informatiesysteem. De medewerker op wie de controle van toepassing is, wordt vooraf hierover geïnformeerd.

Artikel 5 Gerichte controle

1. Gerichte controle kan plaatsvinden indien:
   a een medewerker wordt verdacht van het overtreden van bepalingen uit deze regeling;
   b sprake is van zwaarwegende redenen;
   c dit wettelijk verplicht is; of
   d sprake is van een redelijk vermoeden van een integriteitschending.

2. Gerichte controles kunnen de inhoud van bestanden of berichtenverkeer betreffen en kunnen uitsluitend plaatsvinden gedurende een vastgestelde periode en in opdracht van de algemeen directeur, na advies van de Integriteitsfunctionaris en de CIO. Privé-bestanden worden hierbij zoveel mogelijk ontzien.
3. Gerichte controles kunnen tevens plaatsvinden in opdracht van de CIO en/of de FG in het kader van het in artikel 7, eerste lid, onderdeel h, bedoeld beheer van de ICT-middelen.
4. Gerichte controle wordt slechts uitgevoerd nadat de medewerker is ingelicht dat signalen over hem zijn ontvangen die aanleiding geven tot een gerichte controle.
5. De algemeen directeur kan de inlichtingenplicht, bedoeld in het vierde lid, buiten beschouwing laten voor zover dit noodzakelijk is voor de in artikel 41 van de Uitvoeringswet AVG genoemde belangen. In dat geval wordt de medewerker zo spoedig mogelijk geïnformeerd over de gerichte controle.
6. De algemeen directeur kan, gehoord het in het tweede lid bedoelde advies, besluiten tot het apart plaatsen van bestanden of e-mailboxen om nader onderzoek mogelijk te maken. Hij verwijdert daaruit direct alle niet relevante informatie.

Artikel 6 Maatregelen

1. Indien een medewerker deze regeling niet naleeft, kunnen ordemaatregelen of andere soorten maatregelen worden getroffen.
2. De te treffen maatregel is afhankelijk van de ernst van de overtreding.

Artikel 7 De verwerking van persoonsgegevens van medewerkers

1. De verwerking van persoonsgegevens bij het gebruik van ICT-middelen en VRR-informatie heeft de volgende doeleinden:
   a het verkrijgen van inzicht in de aard en mate van het gebruik van de ICT-middelen en VRR-informatie;
   b het voorkomen van onrechtmatig gebruik dan wel misbruik van de ICT-middelen en VRR-informatie;
   c het beveiligen van de ICT infrastructuur;
   d het beschermen van de privacy van de medewerkers op de werkplek en andere betrokkenen;
   e het beschermen van de integriteit en goede naam van de VRR;
   f het beschermen van de VRR-panden;
   g het nemen van maatregelen bij integriteitsschendingen;
   h het beheer van de ICT-middelen en toegang tot de VRR-informatie;
   i kostenbeheersing bij het gebruik van ICT-middelen;
   j continuïteit van werkzaamheden.

2. Van medewerkers kunnen de navolgende persoonsgegevens worden verwerkt, voor zover noodzakelijk voor de in het eerste lid genoemde doelen:

a geautomatiseerd verkregen logginggegevens;
b naam en zakelijke persoonsgegevens bij incidentmeldingen;
c locatiegegevens van de externe of mobiele werkplek;
d autorisatiegegevens;
e informatie over ter beschikking gestelde ICT-middelen en VRR-informatie;
f informatie over het gebruik van ICT-middelen en VRR-informatie;
g kosten van het gebruik van ICT-middelen;
h informatie over het e-mailverkeer en social mediaverkeer vanuit VRR-accounts.

3. De algemeen directeur treft de nodige maatregelen opdat de verwerking van persoonsgegevens plaatsvindt conform de regels van de AVG. Dit betreft met name maatregelen:
   a die erop zijn gericht dat de persoonsgegevens juist en nauwkeurig zijn;
   b die de persoonsgegevens beveiligen;
   c voor het goede beheer van de persoonsgegevens.

4. De bewaartermijn van persoonsgegevens is in beginsel zes maanden. Persoonsgegevens die ouder zijn, worden verwijderd, tenzij er bijzondere redenen zijn om de gegevens langer te bewaren.
5. Indien gegevens, bedoeld in het vierde lid, langer worden bewaard, wordt de medewerker hierover geïnformeerd vóór het ingaan van de verlenging van de bewaartermijn.
6. Indien de functionaris die belast is met het beheer van de bestanden, delen daarvan niet kan verwijderen, wordt onder verwijderen verstaan het niet meer verstrekken van deze gegevens voor de in het eerste lid geformuleerde doeleinden.

Artikel 8 Rechten van de medewerker

1. De medewerker heeft het recht op informatie over het feit dat van hem persoonsgegevens worden verwerkt.
2. De medewerker heeft het recht om een kopie van een overzicht te ontvangen van de hem betreffende persoonsgegevens die worden verwerkt.
3. De medewerker heeft het recht op rectificatie en aanvulling indien de betreffende persoonsgegevens onjuist of onvolledig zijn.
4. De medewerker heeft het recht op verwijdering of beperking van zijn persoonsgegevens indien de gegevens niet langer nodig zijn voor het doel waarvoor ze worden verwerkt, indien de gegevens onrechtmatig worden verwerkt of indien hij bezwaar maakt of zijn toestemming intrekt terwijl er geen gerechtvaardigde doelen voor verwerking bestaan.
5. De medewerker heeft te allen tijde het recht om bezwaar in de zin van artikel 21 AVG te maken tegen de verwerking van zijn persoonsgegevens, als bedoeld in artikel 7, vanwege met zijn specifieke situatie verband houdende redenen.
6. De medewerker kan een schriftelijk verzoek tot inzage, rectificatie, aanvulling, verwijdering of beperking indienen bij de algemeen directeur.
7. De algemeen directeur bericht de medewerker direct en in ieder geval binnen een maand na ontvangst van een bezwaar als bedoeld in het vijfde lid of een verzoek als bedoeld in het zesde lid, of hij aan het bezwaar of het verzoek tegemoet komt. Afhankelijk van de complexiteit van het verzoek en van het aantal verzoeken kan die termijn indien nodig met twee maanden worden verlengd. Een weigering is met redenen omkleed.
8. De algemeen directeur draagt er zorg voor dat een beslissing op bezwaar of een beslissing tot inzage, rectificatie, aanvulling, verwijdering of beperking zo spoedig mogelijk wordt uitgevoerd.
9. Indien een medewerker het niet eens is met de beslissing van de algemeen directeur kan hij op grond van artikel 77 AVG een klacht indienen bij de Autoriteit Persoonsgegevens.

Artikel 9 Onvoorziene omstandigheden

In gevallen waarin deze regeling niet voorziet of bij twijfel over de toepasselijkheid van deze regeling, beslist de algemeen directeur.

Artikel 10 Openbaarmaking

De algemeen directeur stelt de medewerkers die gebruik maken van de ICT-middelen en VRR-informatie op de hoogte van deze regeling.

Artikel 11 Intrekking oude regeling

De Regeling ICT- en informatiegebruik 2012 wordt ingetrokken.

Artikel 12 Citeertitel en inwerkingtreding

Deze regeling wordt aangehaald als: Regeling ICT- en informatiegebruik VRR 2023 en treedt in werking de dag na publicatie in het blad gemeenschappelijke regeling.

Aldus vastgesteld in de vergadering van 21 juni 2023.

De secretaris,
A. Littooij

De voorzitter,
A. Aboutaleb

Toelichting regeling ICT- en informatiegebruik
Algemeen

Het doel van deze regeling is om:
• het niet aan werk gerelateerd gebruik van door de VRR beschikbaar gestelde voorzieningen te begrenzen;
• het beschermen en beveiligen van systemen en informatie van de VRR;
• de persoonlijke levenssfeer van betrokkenen waarvan persoonsgegevens zijn opgenomen in een of meer persoonsgegevensverwerkingen te beschermen tegen misbruik van die gegevens en tegen opslag van onjuiste gegevens;
• te voorkomen dat persoonsgegevens die in een persoonsgegevensverwerking zijn opgenomen voor een ander doel worden gebruikt dan waarvoor deze bestemd zijn.

De digitale werkomgeving biedt medewerkers mogelijkheden die een zeker risicobesef vragen. Deze regeling bevat daarom regels over de gebruiksmogelijkheden van de digitale werkomgeving, het online gedrag en een bewuste omgang met de risico's.

De regeling is een uitwerking van goed ambtenaarschap en wat de maatschappij mag verwachten van een medewerker van de VRR. Medewerkers moeten zich hieraan houden en zijn hierop aanspreekbaar. In eerste instantie zal de leidinggevende samen met het Hoofd ICT toezien op de naleving van de regeling. Daarnaast vinden controles plaats. Niet naleving van deze regeling kan leiden tot maatregelen.

De regeling beschrijft het gewenste gedrag van de medewerker bij het gebruik van de digitale werkomgeving en VRR-informatie. Ook de VRR als werkgever is aan regels gebonden: goed werkgeverschap en bescherming van de persoonlijke levenssfeer zijn van belang.

De eigen verantwoordelijkheid van medewerkers
Voor de medewerkers gaat het niet alleen om wat mag en niet mag: van groot belang is ook de eigen verantwoorde-lijkheid van de medewerkers. Hiervoor wordt verwezen naar de daartoe opgestelde regels.

Informatiegebruik en -beveiliging onder het flexibel werken.
Het flexibel werken, plaats- en tijdonafhankelijk, is steeds in ontwikkeling en vraagt continue aandacht voor informatiebeveiliging. Beveiligingsrisico's zijn er op verschillende vlakken:

Mens
Het gedrag van de mens is vaak de zwakste schakel. Apparaten kunnen onbeheerd achtergelaten worden, een PC wordt soms niet goed beheerd en kan besmet zijn met malware of virussen. Datadragers (USB-sticks, CD-roms) kunnen kwijtraken. Een bericht kan naar een verkeerde ontvanger worden gestuurd.

Toegang tot informatie
De toegang tot informatie en bedrijfsapplicaties is op afstand beschikbaar gesteld. Toegang met alleen naam en wachtwoord is eenvoudig te kraken.

Locatie
Openbare locaties (bijvoorbeeld horecagelegenheden, flexibele kantoorgebouwen) vergroten het risico op mee-luisteren of meekijken door kwaadwillenden. Niet zakelijke ICT- middelen kunnen onveilig zijn.

ICT-middelen
Voor bijvoorbeeld laptops en PC's geldt dat huisgenoten kunnen meekijken en mogelijk zelfs kunnen inloggen.
ThuisPC's kunnen in een lokaal netwerk zijn opgenomen en benaderd worden vanaf een andere werkplek, mogelijk zelfs via een onbeveiligde draadloze verbinding. Bij verlies of afvoer van oude apparatuur kan data achterblijven en worden achterhaald.

Verbindingen
De verbindingen, als WiFi, kunnen worden afgeluisterd en data kan worden onderschept.

Ofschoon de risico's nieuw lijken zijn er geen principiële verschillen tussen:
- toegang en gebruik van informatie binnen of buiten de kantooromgeving;
- digitaal gebruik of gebruik van analoog/papieren dossier.

Het is in de kern dus de feitelijke context waarin organisatie en medewerkers weer nieuwe antwoorden moeten vinden. Hierbij is het zaak dat ieder zich bewust is van de risico's en daarin ook nadrukkelijk de eigen verantwoordelijkheid neemt. Dit geldt voor de organisatie, die beveiligingsmaatregelen moet nemen en kaders moet stellen, en voor medewerkers, die de maatregelen en kaders in acht moeten nemen en attent moeten blijven op de bestaande beveiligingsrisico's.

Artikelsgewijze toelichting
Hieronder volgt een toelichting op een aantal artikelen.

Artikel 1 Begripsbepalingen
Beveiligingsincident
Hier wordt de integriteit van de gegevens en niet de integriteit van de medewerker of organisatie bedoeld.

Elektronische informatie- en communicatiefaciliteiten
Met sociale media wordt gedoeld op toepassingen als WhatsApp, Facebook, Twitter, LinkedIn, YouTube, Instagram en alle vergelijkbare communicatie toepassingen. Ook blogs, forums en reacties op interne en externe websites vallen hieronder.

VRR-informatie
Hiermee wordt bedoeld alle informatie die de medewerker beschikbaar heeft of bewerkt voor het uitvoeren van zijn functie voor de VRR. Ook informatie waar de medewerker toegang toe heeft maar welke niet nodig is voor de uitvoering van zijn functie valt onder dit begrip.

De informatie kan zich bevinden in een systeem of in ongestructureerde vorm bestaan zoals in documenten, audio en beeld, e-mails en social mediaberichten of op websites van de VRR. Zo valt bijvoorbeeld een WhatsApp bericht aan collega's over een dossier, ook als die met een privé-telefoon is verzonden, onder het begrip VRR-informatie.

ICT-middelen
In de definities wordt onderscheid gemaakt tussen ICT-apparatuur (bijv. computer, laptop, telefoon, tablet) en elektronische informatie en communicatiemiddelen. De ICT-apparatuur omvat ook de daarop geplaatste software en bestanden. Alles tezamen wordt aangeduid als ICT-middelen.

Medewerker
Onder 'degene die betaalde of niet betaalde werkzaamheden voor (een onderdeel van) de VRR verricht' wordt onder andere verstaan: een externe medewerker, een stagiair en een vrijwilliger.

Artikel 2 Gebruik van ICT-middelen en VRR-informatie
De werkgever kan op basis van zijn gezagsbevoegdheid voorwaarden stellen aan het gebruik van ICT-middelen en informatie of bepaalde soorten gebruik verbieden.

Artikel 2, lid 2
Het verbod om de ICT-middelen aan een ander ter beschikking te stellen, betreft zowel betaald als onbetaald ter beschikking stellen. Het is vanzelfsprekend wel toegestaan om de telefoon en dergelijke onder toezicht even te laten gebruiken door een collega.

Artikel 2, lid 6
Medewerkers mogen bij de uitvoering van hun functie gebruik maken van privé ICT-middelen. Denk hierbij aan mobiele (privé)apparatuur en aan het werken vanuit huis. De medewerker heeft de verantwoordelijkheid om bij het gebruik van privé ICT-middelen de voorschriften uit deze regeling in acht te nemen.

Concreet gaat het om het tegengaan van ongewenst gebruik, het zorgen voor goede beveiligingsmaatregelen, het voorkomen van een onnodige belasting van het netwerk en meewerken aan controles. Dit geldt ook in het geval dat de medewerker bij uitvoering van zijn functie gebruik maakt van een privé ICT-middel waar hij geen eigenaar van is.

Artikel 2, lid 7
De medewerker heeft een eigen verantwoordelijkheid om te voorkomen dat er VRR-informatie verloren gaat door het gebruik van (privé) mobiele ICT-middelen. Het gaat hierbij om gebruik van bijvoorbeeld WhatsApp, Facebook, Twitter, LinkedIn, YouTube, Instagram en alle vergelijkbare communicatietoepassingen.

Een social media bericht dat is opgesteld uit hoofde van een functie bij de VRR, is VRR-informatie. Dit is ongeacht met welk account of welk social media platform het bericht is verstuurd of ontvangen en waar het social media bericht wordt bewaard.

Artikel 2, lid 8
In het achtste lid wordt het ongewenst gebruik omschreven. Dit is geen uitputtende opsomming.

Artikel 2, lid 10

Waar het achtste en negende lid vooral zien op de inhoud van de -ongewenste- informatie, ziet het tiende lid vooral op risico's en belasting van het netwerk. Hierbij valt te denken aan het downloaden van te omvangrijke bestanden, het versturen van een mail aan een te grote groep van tegelijk geadresseerden of het geautomatiseerd doorsturen van een mail naar een extern e-mailadres. Ook het privé mailadres is een extern e-mailadres.

Artikel 2, lid 12
Zorgvuldigheid en integriteit zijn de kernbegrippen van het gebruik. De boodschap is eenvoudig en veelomvattend: ga zorgvuldig om met de ICT-middelen en de informatie van de VRR. Deze zorgvuldigheid is vergelijkbaar met begrippen als "goed medewerker". Onderdeel van deze zorgvuldigheid is het bepaalde in het dertiende lid waarin is opgenomen dat medewerkers het privacy- en informatiebeveiligingsbeleid in acht nemen.

De zorgvuldigheid geldt zeker ook voor het gebruik van sociale media, e-mail-, internet- en telefoonfaciliteiten (zoals Whatsapp, SMS en alle vergelijkbare communicatietoepassingen). De medewerker gaat hier verstandig mee om, is transparant over diens betrokkenheid bij de VRR en meldt negatieve berichtgeving bij de leidinggevende.

Artikel 2, lid 13
Het dertiende lid ziet op de beveiliging als onderdeel van de gebruiksnormen. Hier betreft het vooral reeds genomen maatregelen die gerespecteerd moeten worden. Deze gebruiksnormen worden op verschillende momenten en via verschillende kanalen aan de medewerker aangereikt. Daar waar nodig kan ondersteuning of aanvullende opleiding worden aangevraagd. De informatiebeveiligingsaspecten worden verder uitgewerkt in artikel 3.

Artikel 2, lid 15
Als er sprake is van een reis naar een land met een hoog risico op digitale spionage of cybercriminaliteit, is het in beginsel niet toegestaan om ICT-middelen en VRR-informatie mee te nemen of te gebruiken. Tenzij er sprake is van voorgenomen gebruik binnen de Europese Unie vraagt de medewerker bij gebruik van ICT-middelen of VRR-informatie vooraf bij de Servicedesk na of het land waar het gebruik zal plaatsvinden een hoog risico op digitale spionage of cybercriminaliteit heeft. De Servicedesk maakt voor reizen naar die landen een veiligheidsadvies waarin aanwijzingen staan over alternatieve ICT-middelen en waar ter plaatse rekening mee moet worden gehouden. Voorbeelden van hoog risicolanden zijn o.a. China, Rusland en Iran.

Artikel 3 Toegang tot en beveiliging van informatie.
Artikel 3, lid 1
Het eerste lid regelt dat de medewerker alleen die informatie mag benaderen, waarvan hij weet of moet weten dat hij daar toegang tot heeft. Fouten in autorisaties of beveiliging betekenen niet dat de informatie vrij is.

Artikel 3, lid 2
In het tweede lid wordt ingeval van wijziging van functie van de medewerker de verantwoordelijkheid bij de leidinggevende gelegd om de toegang tot VRR-informatie aan te passen. Maar mocht het toch niet goed zijn gegaan dan rust ook op de medewerker de plicht om actie te ondernemen.

Artikel 3, lid 5
De medewerker is verplicht bij gebruik van een privé ICT-middel de VRR-informatie over te dragen. Denk hierbij bijvoorbeeld aan een Woo-verzoek, aan de uitvoering van de Archiefwet 1995 en aan integriteitsonderzoeken.

Artikel 3, lid 6
Met 'de regels die hieromtrent zijn of worden opgesteld' wordt ten tijde van het opstellen van deze Regeling, het VRR Protocol Melding en Afhandeling Datalekken van oktober 2017 bedoeld. Dit protocol is te vinden op intranet.

Artikel 3, lid 7
De algemeen directeur is bevoegd om noodmaatregelen te nemen ingeval van dringende redenen. Uitgangspunt is dat de algemeen directeur deze maatregelen neemt, maar ook de CIO en het Hoofd ICT zijn hiertoe bevoegd. Het Hoofd ICT zal bij afwezigheid vervangen kunnen worden door het Hoofd IM.

Het bovenstaande ziet bijvoorbeeld op de situatie dat vertrouwelijke informatie of gegevens in verkeerde handen dreigen te vallen, doordat bijvoorbeeld een telefoon of laptop is kwijtgeraakt of gestolen. Dan bestaat de mogelijkheid om alle informatie op afstand te wissen. Dit geldt dan ook voor de privé-infor-

matie die op het ICT-middel is opgeslagen. Ook kan een dergelijke noodmaatregel worden toegepast op privé-middelen.

Het spreekt vanzelf dat er voldoende aanleiding moet zijn voor het nemen van een dergelijke maatregel. Dit vergt een afweging door de algemeen directeur. Indien deze niet beschikbaar is, is de CIO respectievelijk het Hoofd ICT hiervoor aangewezen.

De algemeen directeur, de CIO of het Hoofd ICT heeft, indien dit noodzakelijk is, ook de bevoegdheid een account te blokkeren, hetgeen erop neerkomt dat de medewerker zijn werkomgeving niet meer kan benaderen.

Artikel 4 Controle en algemene bepalingen
Artikel 4, lid 1, onder b tot en met d
Controles dienen in redelijke verhouding te staan tot de belangen van de medewerker en de gebruikte middelen mogen niet een verdergaande inbreuk maken op die belangen dan strikt noodzakelijk (proportionaliteit en subsidiariteit). Steeds zal hiertoe een belangenafweging moeten plaatsvinden. Het doel rechtvaardigt dus niet een continue controle en daarmee gepaard gaande verregaande inbreuk op de persoonlijke levenssfeer van de medewerker.

In beginsel zal de controle op naleving slechts steekproefsgewijs en geanonimiseerd mogen geschieden. De uitzonderingen hierop worden uitgewerkt in artikel 5. Indien de (steekproefsgewijze) controle de toegang tot informatie betreft, is het noodzakelijk hierbij authenticatie en/of autorisatiegegevens te betrekken. Deze gegevens zijn niet geanonimiseerd.

Artikel 4, lid 1, onder e
Daar waar de hiervoor genoemde controles slechts beperkte inbreuk op de privacy maken, ligt dit anders indien er sprake is van een redelijk vermoeden van integriteitschending of niet naleven van deze regeling. In dat geval zijn, afhankelijk van de omstandigheden, aanvullende maatregelen noodzakelijk. Het uitgangspunt blijft dat de controle zo beperkt mogelijk wordt gehouden. Indien daartoe zwaarwegende redenen zijn, kan de controle ook gericht plaats-vinden. Dit wordt uitgewerkt in artikel 5 en kan persoonsgegevens en de inhoud van bestanden of berichtenverkeer betreffen.

Artikel 4, lid 2
Controles vragen altijd om een specifieke afweging vooraf. Controles vinden daarom als regel plaats in opdracht van de algemeen directeur. De algemeen directeur omschrijft bij zijn opdracht duidelijk het doel van de controle.

In het kader van het beheer van de ICT-middelen kan ook de CIO opdracht geven voor controle-activiteiten op de ICT-middelen waarover hij het beheer voert. Dit zal echter nooit de inhoud van communicatie of bestanden kunnen betreffen. De algemeen directeur omschrijft bij zijn opdracht duidelijk het doel van de controle.

Artikel 4, lid 6
Controles kunnen ook betrekking hebben op privé ICT-middelen die zakelijk worden gebruikt. De medewerker is verplicht mee te werken aan de controles. Vanzelf spreekt dat daarbij de controleregels van de artikelen 4 en 5 in acht genomen moeten worden, rekening houdend met de eigendomssituatie van de ICT-middelen. Hierbij geldt in het bijzonder dat:
- de doeleinden van de controles beperkingen stellen aan de omvang en wijze van controle (art 4, lid 1); en
- privébestanden zoveel mogelijk worden ontzien (art 4, lid 5).

Artikel 4, lid 7
Geconstateerd kan worden, dat een medewerker zich niet houdt aan de bepalingen van de regeling. Is dat het geval, dan moet de leidinggevende de medewerker hier zo spoedig mogelijk op aanspreken. Een bepaalde tijd voor de opbouw van het dossier is toegestaan indien de omstandigheden daartoe aanleiding geven. Indien de medewerker op zijn handelen in strijd met de regeling wordt aangesproken, is het noodzakelijk dat hij gewaarschuwd wordt voor de (rechtspositionele) gevolgen bij continuering van dit gedrag.

Artikel 4, lid 8
Op grond van artikel 17 van de Wet op de ondernemingsraden hebben de leden van de ondernemingsraad (OR) ten behoeve van hun OR werkzaamheden het recht om onderling te overleggen met gebruik van voorzieningen waarover het OR-lid als zodanig kan beschikken.

Op communicatie van en aan OR-leden in functie zijn de algemene wettelijke regels over vertrouwelijke communicatie van toepassing. Ook de inhoud van het overig ICT-gebruik is geprivilegieerd. Hiervan

mag de algemeen directeur in beginsel geen kennisnemen. Het betreft hier echter geen absoluut verbod. Er kan van worden afgeweken in bepaalde situaties, waarbij men kan denken aan het lekken van geheime of vertrouwelijke stukken.

Artikel 4, lid 9
In sommige systemen zitten controlemechanismen ingebouwd in het kader van informatiebeveiliging en/of ter bescherming van de privacy van burgers. Hier valt bijvoorbeeld te denken aan geautomatiseerde logging in andere systemen. Logginggegevens geven informatie over "het bezoek" aan een bestand: welke gegevens zijn bekeken of opgevraagd etc.

Artikel 5 Gerichte controle
Artikel 5, lid 1
Gerichte controle houdt in dat op persoonsniveau wordt gecontroleerd, waarbij controle op inhoud van e-mail of bestanden kan plaatsvinden. De controles kunnen zijn gericht op:
- een persoon, waartegen concrete verdenkingen bestaan, zoals bijv. signalen van omkoping of fraude; of
- (de oplossing van) een ontstaan probleem, zoals bijvoorbeeld gelekte geheime of vertrouwelijke informatie.

Een gericht onderzoek kan plaatsvinden in het kader van de in artikel 7, eerste lid onder b en e genoemde doelen: het voorkomen van onrechtmatig gebruik dan wel misbruik van de ICT-middelen en VRR-informatie alsmede het beveiligen van het systeem en het netwerk respectievelijk het nemen van maatregelen bij integriteitschendingen.

De beperkingen, genoemd in artikel 4, eerste en tweede lid, zijn hierop van overeenkomstige toepassing:
- de controle wordt zo beperkt mogelijk gehouden (gerichte controle mag niet structureel zijn, maar is altijd tijdelijk);
- de controle moet in een redelijke verhouding staan tot het doel waarvoor deze wordt aangewend (er moet sprake zijn van zwaarwegende belangen van de VRR);
- het doel van de controle moet vooraf duidelijk worden omschreven.

Ingevolge het eerste lid van artikel 5 vindt gerichte controle slechts plaats indien een medewerker wordt verdacht van het niet naleven van deze regeling of indien er sprake is van een redelijk vermoeden van integriteitschending. Om de zorgvuldigheid hierin te waarborgen regelt het tweede lid dat de controle alleen kan plaatsvinden in opdracht van de algemeen directeur, die hiervoor advies vraagt van de Integriteitsfunctionaris en CIO. Ook moet de FG worden geïnformeerd vanwege zijn toezichthoudende taak op de uitvoering van de privacyregels.

Artikel 5, lid 2 en 3
Het derde lid geeft een uitzondering op het tweede lid: in het kader van het beheer van de ICT-middelen kan ook de CIO opdracht geven voor controle-activiteiten op de ICT-middelen waarover hij het beheer voert. Dit zal echter nooit de inhoud van communicatie of bestanden kunnen betreffen. Indien sprake is van een beveiligingsrisico en/of datalek zullen, indien dat noodzakelijk is, de CIO respectievelijk de FG opdracht kunnen geven tot een dergelijke controle. Ook in deze situaties dient het doel van de controle voorafgaand duidelijk omschreven te worden.

Artikel 5, lid 4 en 5
Vindt gerichte controle plaats, dan dient de betrokken medewerker ingevolge lid 4 vooraf te worden geïnformeerd en om zijn reactie gevraagd.

Deze informatieplicht kan volgens art. 41 Uitvoeringswet AVG worden opgeschort voor zover dit noodzakelijk en evenredig is ter waarborging van:
a. de nationale veiligheid;
b. landsverdediging;
c. de openbare veiligheid;
d. de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;
e. andere belangrijke doelstellingen van algemeen belang van de Europese Unie of van Nederland, met name een belangrijk economisch of financieel belang van de Europese Unie of van Nederland, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;
f. de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;
g. de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;

h. een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de gevallen, bedoeld in de onderdelen a, b, c, d, e en g;
i. de bescherming van de betrokkene of van de rechten en vrijheden van anderen; of
j. de inning van civielrechtelijke vorderingen.

Het noodzakelijkheids- en evenredigheidsvereiste van artikel 41 AVG dwingt tot een expliciete afweging ingeval niet vooraf wordt geïnformeerd. In dat geval moet altijd achteraf worden geïnformeerd dat een onderzoek heeft plaatsgevonden. (Ook indien bij het onderzoek geen afwijkingen zijn geconstateerd!)

Bij integriteitsonderzoeken kan het noodzakelijk zijn om bestanden (bijv. ook e mailboxen) tijdelijk apart te plaatsen om nader onderzoek mogelijk te maken.

Artikel 7 De verwerking van persoonsgegevens van medewerkers.
Artikel 7, lid 1
Vanwege privacy vereisten is het noodzakelijk om de doelen van het verwerken van persoonsgegevens en het uitvoeren van controles vooraf vast te stellen. In het eerste lid wordt aan deze eisen voldaan.

Artikel 7, lid 2
Voor wat betreft de informatie over het gebruik van ICT-middelen verdient vooral het gebruik van communicatiefaciliteiten aandacht. Denk bijvoorbeeld aan alle bezochte internetadressen die worden vastgelegd of een telefoonregistratie die alle telefoonnummers bevat. Dit betreft veelal geautomatiseerd verwerkte gegevens, die in eerste aanleg alleen verkeersgegevens betreffen (dus welke IP-adressen van computers of welke telefoonnummers), Koppeling van deze verkeersgegevens aan een persoon is echter een mogelijkheid, bijvoorbeeld in het kader van gerichte controle.

Ook e-mail en WhatsApp verkeer (en die van andere vergelijkbare producten) valt onder de opsomming. Dit betreft niet alleen de verkeersgegevens hiervan, maar mogelijk ook de inhoud van de mails of bijvoorbeeld WhatsApp berichten. Vanzelf spreekt dat privé berichten zo veel als mogelijk worden ontzien.

Artikel 7, lid 4
Het is in het algemeen niet nodig om de persoonsgegevens lang te bewaren. De standaardtermijn is zes maanden.

In het geval van een zwaarwegend vermoeden van onrechtmatig gebruik dan wel misbruik van ICT-middelen en VRR-informatie of in geval van een integriteitsschending worden de gegevens bewaard zolang dit in het kader van nader onderzoek en eventueel te treffen maatregelen jegens een medewerker noodzakelijk is. Zodra een nader onderzoek is afgerond en dit niet leidt tot maatregelen jegens een medewerker worden de gegevens verwijderd.

Artikel 7, lid 6
Bepaalde gegevens kunnen soms om technische redenen niet worden verwijderd. Van het e-mailsysteem worden bijvoorbeeld back-ups gemaakt die in geval van nood teruggezet kunnen worden. Deze back-ups kunnen niet zonder meer gewist worden. Het is ook niet mogelijk om binnen een dergelijke back-up een individueel e mailbericht te verwijderen. De bedoelde gegevens mogen in deze gevallen niet meer worden verstrekt (verwerkt).

Artikel 8 Rechten van de medewerker.
In dit artikel worden de rechten van de medewerkers bij het verwerken van persoonsgegevens behandeld. De rechten van betrokkenen worden geregeld in de artikelen 12 tot en met 22 AVG. De rechten van de medewerker kunnen buiten toepassing gelaten worden in bijzondere omstandigheden als vastgelegd in artikel 41 van de Uitvoeringswet AVG. Bijvoorbeeld indien dat nodig is in het belang van de voorkoming, opsporing en vervolging van strafbare feiten.

Het recht op beperking houdt in dat de persoonsgegevens (tijdelijk) niet verwerkt mogen worden en niet gewijzigd mogen worden.

Een medewerker die het niet eens is met de verwerking van zijn persoonsgegevens kan daartegen bezwaar maken bij de algemeen directeur. Indien een medewerker het niet eens is met de beslissing van de algemeen directeur kan hij op grond van artikel 77 AVG een klacht indienen bij de Autoriteit Persoonsgegevens.