Veiligheidsregio Groningen

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 386

20 februari 2025

Officiële uitgave van de gemeenschappelijke regeling Veiligheidsregio Groningen

Gedragscode Informatiebeveiliging & Privacy

A. Uitgangspunten van de gedragscode

Veiligheid zit in de cultuur van Veiligheidsregio Groningen (hierna VRG). Onze missie: “Samen werken we aan veiligheid. Iedere dag, steeds beter. Dat doen we professioneel en daadkrachtig, betrouwbaar en verbonden.” Dit geldt ook voor onze (digitale) werkomgeving. Om op organisatieniveau een solide fundament op het gebied van informatieveiligheid en privacy te bouwen, hebben we omschreven hoe we binnen de VRG omgaan met onze bedrijfsmiddelen en hoe we veilig omgaan met informatie en persoonsgegevens. Van medewerkers van de VRG en anderen werkzaam voor de VRG wordt verwacht dat zij verantwoord omgaan met de beschikbaar ge-stelde bedrijfsmiddelen en veilig omgaan met informatie en persoonsgegevens.

De gedragscode is een toetsingskader voor het gewenste gedrag omtrent informatiebeveiliging en privacy. Van-uit informatiebeveiliging en privacy wil de VRG haar medewerkers handvatten bieden om verantwoord en veilig gebruik te maken van de digitale middelen binnen onze werkomgeving. Waarbij de privacy van alle medewer-kers en in de organisatie betrokken personen (zowel in- en externen) optimaal is geborgd, dit in overeenstem-ming met de juridische kaders (o.a. Baseline Informatieveiligheid Overheid en AVG-wetgeving).

De gedragscode legt regels vast voor het gebruik van bedrijfsmiddelen door medewerkers. En over de controle op de naleving hiervan. Onder bedrijfsmiddelen worden in ieder geval verstaan de (ICT)faciliteiten en verschil-lende gegevens, waaronder: hardware (computer, laptop, tablet, telefoon, toegangspas/-druppel), software (of- systemen), informatie en (persoons)gegevens en internetgebruik.

B. De gedragscode

Reikwijdte

1. Deze gedragscode is van toepassing op alle personen in dienst van de VRG en personen die (betaalde of on-betaalde) werkzaamheden voor de VRG verrichten, zoals ingehuurd personeel of stagiairs.
2. De gedragscode is tevens van toepassing op alle verwerkingen van persoonsgegevens van en door personen in dienst van de VRG en personen die (betaalde of onbetaalde) werkzaamheden voor de VRG verrichten, zoals ingehuurd personeel of stagiairs.

C. Gebruik van apparaten en systemen

In de onderstaande hoofstukken staat beschreven op welke manier wij als de VRG omgaan met onze apparaten.

Artikel 1 Gebruik van elektronische apparaten

1. Privégebruik van de elektronische communicatiemiddelen is toegestaan mits dit gebruik in overeenstem-ming is met deze regeling en dit gebruik in geen geval storend is voor dan wel ten koste gaat van het uitvoe-ren van de werkzaamheden voor de VRG.
2. Bij het gebruik van door de VRG beschikbaar gestelde apparatuur verwacht de VRG van alle medewerkers dat zij netjes en zorgvuldig met deze middelen omgaan;
   - Apparatuur wordt buiten beschermd vervoerd (dit bijvoorbeeld in een beschermhoes of tas).
   - Schade, diefstal of verlies wordt zo spoedig mogelijk gemeld bij de Servicedesk.
     - Buiten kantoortijden wordt diefstal of verlies zo spoedig mogelijk gemeld bij de Cyberweerbaarheidsdienst, om te voorkomen dat eventuele kwaadwillenden bij VRG-gegevens kunnen.

3. Verbindingen worden alleen gemaakt met een beveiligd WIFI-netwerk (inlog en wachtwoord) of een bevei-ligde hotspot vanaf een vertrouwde mobiele bundel;
   - Gebruik van onbeveiligde openbare WIFI-netwerken is niet toegestaan.
     - Indien nodig kan de persoonlijke databundel op het VRG toestel dienen als hotspot, dit in beperkte mate tot max 5 GB per maand.

4. Verdachte e-mails die worden ontvangen of (per abuis) worden aangeklikt:
   - Worden gemeld bij Security/Privacy medewerkers, cyberweerbaarheidsdienst of PI@vrgroningen.nl.
   - Als gewaarschuwd wordt voor een cyberdreiging of -aanval, dient de aanwijzingen van de CISO, Security & Privacy Officer, cyberweerbaarheidsdienst of PI@vrgroningen.nl te worden opgevolgd.

Artikel 2 Aanschaf van apparatuur

1. Aanschaf van apparatuur vindt plaats in afstemming met IM/ICT (let op, het gaat hier niet om aanschaf appa-ratuur voor thuiswerkplek, voor afspraken hierover zie VRGnet 'mijn thuiswerkplek');
   - Apparatuur wordt voorzien van een unieke code en opgenomen in het apparatuur overzicht (CMDB) van IM/ICT.

2. De aankoop moet passen bij de integriteit van onze organisatie, waardoor bedrijfsmiddelen niet in strijd mogen zijn met wet- en regelgeving. Een DPIA wordt uitgevoerd voor elke nieuwe aanschaf, wat helpt om privacy te kunnen waarborgen. Zie artikel 15 voor meer details over dit proces.

Artikel 3 Stel informatie veilig

Zowel op kantoor, bij het gebruik van de printer, op de thuiswerkplek maar ook op een andere locatie waarbij je gebruik maakt van informatie van de VRG, zorg je dat je informatie nooit onbeheerd achterlaat. De VRG hanteert hiervoor de volgende richtlijnen:

1. Verwijder interne en vertrouwelijke documenten van het bureau bij het verlaten van de werkplek en leg deze in een afgesloten kast of tas;
2. Vergrendel bij het (tijdelijk) verlaten van de werkplek de pc;
3. Verwijder informatie van muren en borden, wanneer deze informatie geen doel meer heeft;
4. Gooi overbodig geworden papieren documenten met persoonsgegevens altijd weg in de hiervoor bestem-de archiefvernietigingsbakken (grijze bakken die zijn voorzien van een gleuf voor papier);
5. Het gebruik van USB Stick/harddisk zijn niet toegestaan, tenzij in overleg met IM/ICT;
6. Laat geen afdrukken bij de printer liggen, zeker niet als er persoonsgegevens op staan;
7. Log altijd uit bij de printer wanneer je klaar bent met kopiëren, scannen of overige opdrachten.

Artikel 4 Toegangsbeveiliging en toegangspas/-druppel

1. Medewerkers beschikken over een toegangspas/-druppel;
   - De pas wordt onder geen enkele omstandigheid uitgeleend aan een ander;
   - Extra rechten worden aangevraagd bij de Servicedesk of medewerker Brandweerzorg

2. Bij het vergeten van de pas/druppel:
   - Ontvangt de medewerker een tijdelijke toegangspas/-druppel.

3. Verloren passen/druppels:
   - Worden zo spoedig mogelijk gemeld bij de Servicedesk of medewerker Brandweerzorg;
   - De rechten worden ingetrokken en de druppel geblokkeerd;

4. Medewerkers zijn zelf verantwoordelijk om gasten op te halen uit de ontvangsthal en deze na afloop van het overleg ook weer te begeleiden naar de ontvangsthal bij de Servicedesk;
5. Bij twijfel of een persoon een medewerker of te gast is:
   - Vraagt de persoon in kwestie wie diegene is.
     - Als dit ongeloofwaardig overkomt, meldt men dit bij de Servicedesk.

6. Gasten die zich bevinden in ruimtes waartoe zij niet behoren:
   - Aanspreken waarom de gast zich bevindt in de betreffende ruimte;
   - Neem contact op met de Servicedesk.

D. Informatieveiligheid

Informatieveiligheid (er)kent diverse dreigingen die gericht zijn op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. In de onderstaande hoofstukken staat beschreven op welke manier wij als VRG omgaan met informatieveiligheid.

Artikel 5 E-learning informatieveiligheid en privacy

1. Elke medewerker behoort maximaal 3 maanden na indiensttreding de E-learning behaald te hebben;
2. Om de vaardigheden up-to-date te houden wordt de medewerker periodiek getoetst op zijn/haar (digitale) vaardigheden op het gebied van informatieveiligheid en privacy.

Artikel 6 Wachtwoordgebruik en Multi factor authenticatie (MFA)

1. De VRG maakt gebruikt van Multifactor Authenticatie (MFA). Om gebruik te kunnen maken van de werk-plekomgeving van de VRG, moet naast inlognaam en wachtwoord ook via SMS/Authenticator app een inlog-verzoek worden goedgekeurd. Elke medewerker behoort zijn/haar eigen MFA in te stellen.
2. Een wachtwoord is persoonsgebonden en mag onder geen enkele voorwaarde worden verstrekt aan ande-ren in welke zin of functie dan ook. Bij VRG gelden de volgende afspraken voor wachtwoordgebruik:
   - Een wachtwoord van een persoonsgebonden account met normale bevoegdheden;
     - Moet uit minimaal 8 tekens bestaan (hoe meer hoe sterker het wachtwoord);
     - Moet tenminste één letter, één cijfer en één leesteken bevatten;
     - Mag niet hetzelfde zijn als de loginnaam (of de accountnaam);
     - Mag niet hetzelfde zijn als de 10 wachtwoorden die daarvoor zijn gebruikt.

3. Nieuw verstrekte wachtwoorden moeten zo snel mogelijk, maar uiterlijk binnen een maand, worden aange-past. De nieuw verstrekte wachtwoorden vervallen bij het niet voldoen aan deze verplichting binnen een maand.

Artikel 7 Gebruik van OneDrive en SharePoint

1. OneDrive is een persoonlijke werkomgeving waartoe andere medewerkers geen toegang hebben. Data die op deze omgeving wordt opgeslagen is enkel werk gerelateerd. Bij uitdiensttreding wordt na 90 dagen de data definitief verwijderd.
2. SharePoint is een gezamenlijke werkomgeving waartoe medewerkers wiens toegang zijn gegeven tot een site, map, bestand, document of gegevens om dit te raadplegen of te bewerken. Daarnaast is het uitgangs-punt om grote bestanden (met externen) te delen via een SharePointsite (niet via Outlook).
   - Delen en toegankelijk maken van documentatie is op basis van nut en noodzaak (rol en functie);
   - Toegang (intern/extern) tot een site wordt aangevraagd bij IM/ICT.

Artikel 8 Gebruik van e-mail

1. De VRG-mail(box) wordt uitsluitend voor werk gerelateerde doeleinden gebruikt;
2. Het automatisch doorsturen van werk gerelateerde mailberichten naar de privémail is niet toegestaan;
3. De mailbox is niet bedoeld als archief voor bijvoorbeeld via de mail ontvangen bijlages. Persoonlijke werk gerelateerde bijlagen worden zo veel mogelijk opgeslagen in OneDrive, gedeelde bijlagen worden opgesla-gen op SharePoint;
4. De optie ‘allen beantwoorden’ wordt alleen gebruikt als de noodzaak daarvoor aanwezig is;
5. Racistische, seksueel intimiderende, discriminerende of anderszins beledigende/ongepaste uitingen zijn niet toegestaan.

Artikel 9 Gebruik van internet

1. Incidenteel persoonlijk gebruik is toegestaan, mits dit:
   - Niet storend is voor de dagelijkse werkzaamheden, niet voor commerciële doeleinden is en geen verboden gebruik oplevert, zoals onder art. 11.2 staat beschreven.

2. Het is niet toegestaan om:
   - Internetsites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootge-vend materiaal bevatten;
   - Films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van een il-legale bron;
   - Medewerkers lastig te vallen of te pesten;
   - Deel te nemen aan kansspelen;
   - Ander ongewenst gedrag te vertonen.

Artikel 10 Gebruik van applicaties

1. Applicaties worden gedownload vanuit:
   - De standaard store op de bedrijfslaptop;
   - Bedrijfsportal of standaard store van de bedrijfstelefoon;
   - Overige downloadomgeving op aanvraag bij IM/ICT.

2. Applicaties worden uitsluitend gebruikt:
   - Om werkzaamheden uit te voeren en werk gerelateerde platformen te raadplegen.

3. Applicaties worden uitsluitend gebruikt ter uitoefening van werkzaamheden;
   - Games, video en streamdiensten zijn niet toegestaan.

Artikel 11 Gebruik sociale media

1. De officiële (social)mediakanalen van VRG worden uitsluitend gebruikt door bestuursleden, directie en woordvoerders van VRG (die hiervoor geautoriseerd zijn);
2. Accounts op sociale applicaties zijn niet gekoppeld aan of (in)direct verbonden met het VRG e-mailadres;
3. Zonder voorafgaande toestemming mogen geen persoonsgegevens (foto's of gegevens) van collega's op sociale media worden geplaatst;

E. Privacy

De privacywetgeving (algemene verordening gegevensbescherming, AVG) stelt dat elke medewerker, zowel dagdienstmedewerker, beroeps als vrijwilliger, zorgvuldig omgaat met persoonsgegevens. Van medewerkers wordt verwacht dat zij zorgvuldig omgaan met informatie, in het bijzonder persoonsgegevens. Dat zij de priva-cywetgeving hanteren bij uitvoering van dagelijkse werkzaamheden en op geen enkele wijze informatie, waar-van redelijkerwijze kan worden aangenomen dat deze vertrouwelijk of privacygevoelig is, zonder toestemming van betrokkene of leidinggevende te gebruiken en/of delen buiten de organisatie. Medewerkers zijn verplicht tot geheimhouding van hetgeen hen in verband met hun functie ter kennis is gekomen, voor zover die verplich-ting uit de aard der zaak volgt.

Voor het werken met persoonsgegevens binnen VRG gelden drie gouden uitgangspunten:

1. Medewerkers gebruiken alleen gegevens als dat nodig is om veilig en goed voorbereid onze werkzaamhe-den uit te voeren, of als het nodig is om de taken van VRG als werkgever uit te voeren. Dit heet **doelbinding**.
2. Medewerkers gebruiken niet meer gegevens dan noodzakelijk is om dat doel te bereiken. Dat betekent ook dat alleen personen die echt iets moeten met de gegevens, daartoe toegang mogen hebben. Dat heet **da-taminimalisatie**.
3. Medewerkers gebruiken alleen gegevens als daarvoor een **wettelijke grondslag** te vinden is. De meest voorkomende zijn een wettelijke verplichting, de uitvoering van een overeenkomst of toestemming.

Artikel 12 Datalekken en het melden

1. Het is belangrijk dat een datalek direct gemeld wordt, wanneer dit wordt geconstateerd. Dit is wettelijk ver-plicht: Een datalek moet gemeld worden bij de Functionaris Gegevensbescherming, Security & Privacy Officer of per mail: PI@vrgroningen.nl. Na het doen van een melding wordt er (direct) actie ondernomen door de Func-tionaris Gegevensbescherming en/of Security & Privacy Officer, zodat eventuele (neven)schade kan worden beperkt.

Artikel 13 Data protection impact assessment (DPIA)

De DPIA is een (wettelijk verplicht) instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen. En om daarna maatregelen te kunnen treffen om de risico's te verkleinen. DPIA's worden uitgevoerd bij projecten, aanbestedingen of nieuwe/veranderende processen waar persoonsgegevens ver-werkt (gaan) worden.

1. De DPIA wordt uitgevoerd door de verantwoordelijke contracteigenaar, proceseigenaar, applicatiesysteembeheerder of projectgroep.
   - Medewerker(s) worden tijdens de uitvoering van de DPIA ondersteund door de Security & Privacy Officer;
   - Uiteindelijk wordt de DPIA getoetst door de Functionaris Gegevensbescherming.

Artikel 14 Verwerkersovereenkomst

Daarnaast is het volgens de AVG-wetgeving een verplichting dat schriftelijk afspraken worden gemaakt en vast-gelegd met leveranciers van (online)applicaties, als hierbij persoonsgegevens worden verwerkt (denk hierbij aan inloggegevens, wachtwoorden en het opslaan van gemaakt werk). Deze afspraken worden (in samenwerking met Juridische Zaken) vastgelegd in een verwerkersovereenkomst. De contracteigenaar (in samenwerking met Juridische Zaken) is verantwoordelijk dat de verwerkersovereenkomst wordt getekend.

Artikel 15 Verwerkingsregister

Daarnaast is het volgens de AVG-wetgeving een verplichting dat een verwerkingsregister wordt bijgehouden voor processen, waarbij persoonsgegevens worden verwerkt.

1. Proceseigenaren zijn verantwoordelijk voor het actualiseren van het verwerkingsregister. Dit kan periodiek of bij wijziging van de verwerking (aanvullende persoonsgegevens of een extra verwerking)
   - Medewerker(s) worden tijdens het actualiseren ondersteund door de Security & Privacy Officer;
   - Periodiek wordt het verwerkingsregister getoetst door de Functionaris Gegevensbescherming.

F. Naleving en disciplinaire maatregelen

Artikel 16 Overtreding

Bij de VRG hechten we veel waarde aan een professionele werkomgeving waarin informatieveiligheid en het (waar)borgen van privacy belangrijk is. Het naleven van de gedragscode is daarbij essentieel. Mocht een mede-werker onverhoopt de gedragscode overtreden, dan spreken we elkaar aan en proberen we een volgende overtreding te voorkomen. We hopen natuurlijk dat dergelijke situaties zeldzaam blijven. Bij de VRG vertrouwen we erop dat iedereen zijn of haar steentje bijdraagt.

Bij overtreding van de gedragscode kunnen verschillende maatregelen worden genomen, afhankelijk van de ernst van de overtreding variërend van een waarschuwing tot serieuzere stappen. Hoofdstuk 16 (disciplinaire straffen) en hoofdstuk 19, paragraaf 8 (Disciplinaire maatregelen schorsing in het belang van de dienst) van de Arbeidsvoorwaardenregeling Veiligheidsregio Groningen zijn hierbij van toepassing.

In gevallen waar schade is ontstaan door schuld of nalatigheid, kan de VRG, conform artikel 15:1:12/19:37 Ar-beidsvoorwaardenregeling Veiligheidsregio Groningen, besluiten dat de medewerker (een deel van) de schade vergoedt.
Bij strafbare feiten zal de VRG, indien nodig, aangifte doen bij de politie om de integriteit van onze organisatie te waarborgen.

Artikel 17 Monitoring en inhoudelijke controle

Monitoring en inhoudelijke controle van het gebruik van ICT-bedrijfsmiddelen kan uitsluitend plaatsvinden voor onderstaande doeleinden:

1. Het voorkomen van onrechtmatig gebruik, dan wel misbruik van ICT-bedrijfsmiddelen;
2. Naleving van de rechtspositieregelingen die de VRG voor haar medewerkers heeft vastgesteld, op vorde-ring van bevoegde instanties en bij vermoeden van schending of overtreding van enige gedragscode;
3. Het beveiligen van onze systemen en het netwerk;
4. Bescherming van vertrouwelijke informatie;
5. Tegengaan/voorkomen van (cyber)pesten;
6. Tegengaan/voorkomen van digitale uitingen (te denken aan discriminatie of seksuele intimidatie);
7. Tegengaan/voorkomen van ongeoorloofde handelingen ten aanzien van één of meerdere medewerkers;
8. Behandelen van geschillen;
9. Bescherming van privacygevoelige informatie.

Controle door VRG op het gebruik van de ICT-middelen vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot individuele personen (beperkt zich tot verkeersgegevens internet en mail). Alleen bij zwaarwegende redenen vindt er controle op de inhoud plaats. De directie van VRG is bevoegd om het besluit te nemen om over te gaan op inhoudelijke controle. De directie van VRG zal dit verzoek neerleg-gen bij de afdeling IM/ICT. De betrokken medewerker wordt hierover geïn-

formeerd door de directe leidingge-vende en in de gelegenheid gesteld persoonlijke gegevens te verwijderen. Aan deze voorwaarde kan in zwaar-wegende gevallen door de werkgever worden voorbijgegaan. Van de medewerker wordt verwacht dat deze medewerking verleent op het moment dat een controle plaatsvindt. VRG kan vervolgens de opdracht geven om persoonsgegevens automatisch en elektronisch vast te leggen vanuit de VRG ingezette software. VRG legt alleen gegevens in een (afgeschermd) incidentregister vast die noodzakelijk zijn voor de doeleinden van de verwer-king (onderzoek). VRG legt de volgende gegevens vast:

1. Gebruikersidentificatie, naam, voornaam of voorletters van de medewerker, code sector of afdeling waar de medewerker onder valt;
2. Toegang tot internet, gebruikersnaam en internetprotocoladres;
   - Datum en het tijdstip van het openen en sluiten van de toegang tot het internet en bezochte inter-netsites/webpagina's (internetprotocoladressen).

3. De datum en het tijdstip van verzenden, dan wel ontvangen van e-mailberichten door de medewerker;
   - De inhoud van de door de medewerker verzonden en ontvangen e-mailberichten (zakelijk en pri-vé).

4. Rechten en privileges;
   - (Toegangen)rechten die behoren tot een account- of functieprofiel.

Persoonsgegevens (n.a.v. onderzoek) worden conform de daarvoor wettelijke vastgestelde termijnen bewaard.

Artikel 18 Personen aan wie persoonsgegevens worden verstrekt
De vastgelegde persoonsgegevens worden, na bewerking, verstrekt aan:

1. Het team IM/ICT om inzicht te verkrijgen in de mate van gebruik van de ICT-bedrijfsmiddelen.
2. De werkgever dan wel de door werkgever aangewezen leidinggevende of andere bij het onderzoek be-trokken personen, indien er een redelijk vermoeden bestaat van onrechtmatig gebruik dan wel misbruik van de elektronische communicatiemiddelen.

Van de uitvoering van het onderzoek wordt een verslag opgemaakt. Dit verslag wordt ter kennisname aan de medewerker en in geanonimiseerde en niet tot een persoon herleidbare vorm aan de OR gezonden.

Artikel 19 Rechten van medewerker
1. Aan de medewerker die daarom aan de werkgever verzoekt, wordt een overzicht verschaft van de hem betreffende persoonsgegevens die worden verwerkt.
2. Degene aan wie overeenkomstig het eerste lid kennis is gegeven van de hem betreffende persoonsgege-vens, kan de werkgever verzoeken deze te verbeteren, aan te vullen, te verwijderen of af te schermen in-dien deze feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn, dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. Het verzoek bevat de aan te brengen wijzigingen.
3. De werkgever bericht de verzoeker binnen vier weken na ontvangst van het in het tweede lid genoemde verzoek schriftelijk of, dan wel in hoeverre hij daaraan voldoet. Een weigering is met redenen omkleed. Een beslissing op een verzoek geldt als een besluit in de zin van artikel 1:3 Algemene wet bestuursrecht en wordt genomen door de directeur van Veiligheidsregio Groningen.
4. De werkgever draagt er zorg voor dat een beslissing tot verbetering, aanvulling, verwijdering of afscher-ming zo spoedig mogelijk wordt uitgevoerd.

G. Overige bepalingen

Artikel 20 Bijzondere gevallen
In gevallen waarin deze regeling niet voorziet of niet naar redelijkheid voorziet, beslist het bestuur.

Artikel 21 Intrekking Regeling privacy en omgang elektronische communicatiemiddelen
De Regeling privacy en omgang elektronische communicatiemiddelen wordt ingetrokken met ingang van de datum van inwerkingtreding van deze regeling.

Artikel 22 Inwerkingtreding
Deze regeling treedt in werking op 24 februari 2025.

Artikel 23 Citeertitel
Deze regeling wordt aangehaald als Gedragscode informatiebeveiliging en privacy.