



aan DB

van 5.1.2.e

onderwerp Gedragsregels digitale werkomgeving CBS

datum 11 juli 2022

1. Inleiding

Zonder onze digitale werkomgeving kunnen we ons werk niet doen. Belangrijke aspecten daarbij zijn informatiebeveiliging en privacy. We werken met persoonsgegevens en andere vertrouwelijke informatie om onze statistieken te kunnen maken en om bedrijfsvoering te kunnen uitvoeren. Het tijdstip waarop en de plek waar we werken is steeds flexibeler. Daarnaast zijn we steeds vaker een doelwit van cybercriminelen met geavanceerde digitale aanvallen gericht op spionage, sabotage en zelfs terrorisme. Zorgvuldig omgaan met informatie betekent dus ook veilig en privacy-verantwoord.

Ons gedrag is daarbij van groot belang. Met technische en organisatorische maatregelen beperken we al veel risico's, maar dat is niet voldoende. Deze gedragsregeling beschrijft wat je geacht wordt te doen om goed om te gaan met informatie zodat die informatie veilig en de privacy gewaarborgd blijft. Door met zijn allen deze regels toe te passen, kunnen we veiliger ons werk doen en worden we digitaal weerbaarder.

Het past bij de eed of belofte waarin je hebt toegezegd om je te gedragen zoals 'een goed ambtenaar betaamt'. Het past ook bij de betrouwbaarheid die de maatschappij van de overheid verwacht. Je houden aan deze regels is dus niet vrijblijvend; die plicht volgt ook uit wet- en regelgeving zoals bijvoorbeeld de CBS-wet, Europese wetgeving voor statistiekbureaus, de Archiefwet, en de Algemene Verordening Gegevensbescherming (AVG). Een fout maken of je vergissen kan iedereen overkomen, maar bij opzet en nalatigheid kan het leiden tot personele maatregelen.

2. Scope

Deze gedragsregeling gaat vooral over digitale informatie en informatiesystemen en om een veilige en privacy verantwoorde manier van werken. Digitaal werken raakt aan het werken met papieren informatie en fysieke beveiliging. Die onderwerpen komen om die reden beperkt aan bod.

Daarnaast zijn binnen het CBS nog een aantal verwante beleidsregels van toepassing, zoals over integriteit, het gebruik van communicatiekanalen en archivering, en [richtlijnen voor CBS-medewerkers op social media](#).



Deze gedragsregeling geldt voor alle personen die bij of voor het CBS werken en gebruik maken van de digitale werkomgeving van het CBS. Dit zijn de eigen medewerkers, uitzendkrachten en andere externen, medewerkers van zakelijke partners, stagiair(e)s, trainees en vrijwilligers.

Beheer van het document:

- In geval de hoofdregels van deze gedragsregeling veranderen, is brede afstemming noodzakelijk en hernieuwde instemming van de OR.
- Tekstuele wijzigingen waarbij een toelichting, een link of een voorbeeld wordt aangepast worden vastgesteld door de Chief Information Officer (CIO) en dan ter informatie naar het DB en OR gestuurd.

3. Eigen verantwoordelijkheid

Iedere CBS'er is zelf verantwoordelijk voor zijn eigen gedrag en de keuzes die hij maakt. Het aan de gedragsregels houden is belangrijk en niet vrijblijvend. Fouten en vergissingen maken is menselijk. Maar als je je niet aan deze regels houdt, kan dat een blijk zijn van disfunctioneren, plichtsverzuim en niet-integer gedrag.

In de drukte van alle dag is het makkelijk om iets te vergeten en een fout te maken. Help elkaar bijvoorbeeld door de computer voor de ander te vergrendelen en vertel hem dat als hij er weer is. Verwijder een e-mail die niet voor jou bedoeld is en meld dit bij de afzender. Als je denkt dat een collega niet weet hoe hij iets moet doen, laat het een keer zien. Door elkaar op die manier te helpen, voorkomen we dat zaken misgaan. Als je dit lastig vindt, zijn er natuurlijk ook andere mogelijkheden om iets aan te kaarten, zoals dit melden bij je leidinggevende of een vertrouwenspersoon.

4. Veilig werken plaats- en tijdonafhankelijk werken

4.1 Op kantoor

Gebruik alleen de door het CBS aan jou verstrekte of voor jou beschikbare ICT-voorzieningen om je werk uit te voeren. Hiermee krijg je toegang tot alle informatie en alle applicaties die je uit hoofde van je functie of rol nodig hebt.

Vergrendel al je apparatuur als je wegloopt van je (thuis) werkplek. Zo voorkom je dat een bezoeker, collega of huisgenoot toegang krijgt tot jouw e-mail, documenten en systemen.

Berg papieren op in een gesloten lade, locker of kast als je je werkplek verlaat en die werkdag daar niet meer terugkomt. Als je op je werkdag een langere tijd van je werkplek weggaat, zorg dan dat je papieren zo geordend of gestapeld zijn dat een langslappende collega of bezoeker geen toegang tot de informatie daaruit krijgt. Op flexplekken zorg je zo dat je collega aan een opgeruimd bureau kan werken.



Vind je printjes van iemand anders bij de printer: geef ze aan de eigenaar of gooi ze in de papiercontainer/papierversnipperaar.

4.2 Thuiswerken

Bijna alle kantoorwerkzaamheden kan je ook thuis doen. Thuiswerken brengt echter ook een extra verantwoordelijkheid met zich mee. Je huisgenoten en gasten van jou en jouw huisgenoten zijn (meestal) geen CBS'er en mogen dus helemaal geen toegang hebben tot de informatie waarover je uit hoofde van je functie beschikt. Op de vestigingen wordt dit (deels) voor je opgevangen doordat personen die rond jouw werkplek rondlopen ten minste – met toestemming van en door het CBS gecheckt – door de fysieke toegangsbeveiliging zijn gekomen. Bij jouw thuis kunnen wij dat niet voor je regelen en zul je dus extra moeten opletten.

Zorg er bijvoorbeeld voor dat je de IT-werkplek thuis vergrendelt en belangrijke documenten opbergt als je wegloopt. Zorg er ook voor dat je thuisnetwerk afdoende beveiligd is, bijvoorbeeld door middel van een toegangsleutel. Voorkom bij overleggen dat iedereen kan meeluisteren.

Als je graag werkt in één van de gemeenschappelijke ruimten (zoals keuken of huiskamer) van je huis is het goed om je werkplek zo op te stellen dat je huisgenoten niet in de verleiding gebracht worden om over je schouder op je scherm te kijken. Mensen zijn nieuwsgierig. Ook jouw huisgenoten. Een aparte (arbo-conforme) werkplek kan daarbij helpen.

4.3 Onderweg

Je kunt de door het CBS verstrekte voorzieningen en apparatuur veilig onderweg gebruiken mits je onderstaande regels in acht neemt. Hiermee kun je je e-mail bekijken en versturen en kun je bij andere zakelijke informatie.

Print zo min mogelijk en werk zoveel mogelijk digitaal. Als je met geprinte documenten of notitieboekjes werkt, is de kans groter dat je deze verliest en de informatie direct zichtbaar is. Je kunt onderweg inloggen op de digitale werkomgeving op je laptop, tablet of telefoon. De thuiswerkomgeving brengt je naar de veilige omgeving van je organisatie.

Maak geen gebruik van openbare wifi-netwerken. Die zijn niet veilig. Werk daarom via vertrouwde wifi, je persoonlijke hotspot of 3G/4G/5G. De CBS-gebouwen zijn voorzien van een veilig wifi-netwerk; werk daarbuiten zo veel mogelijk via VPN of de 4G/5G-simkaart in je telefoon. Je kunt ook je telefoon instellen als een wifi-hotspot om daarmee op je laptop te werken.

Zorg dat anderen niet kunnen meekijken op je scherm. Werk je veelvuldig op openbare plekken, overweeg dan een privacyscherm voor op je beeldscherm (verkrijgbaar via de servicebalie). Ga ervan uit dat je buurman in trein, café of andere openbare plekken meekijkt: mensen zijn nieuwsgierig. Als iemand naast of achter je zit, zorg dan dat je geen vertrouwelijke informatie op je scherm hebt staan.



Bel je in het openbaar? Houd dan afstand tot anderen of stel het gesprek uit. In het openbaar luisteren anderen mee, ook bijvoorbeeld in de lift. Let dus op wat je er bespreekt. Zoek een rustig plekje op en houd afstand tot anderen. Ook kan je aan je gesprekspartner voorstellen om het gesprek later te voeren: niet alles heeft haast.

Buiten Europa: pas op met datagebruik. Als je in overleg met je leidinggevende toch je zakelijke apparatuur meeneemt op vakantie of dienstreis, pas dan op met datagebruik. Binnen de EU gelden dezelfde voorwaarden als in Nederland. Maar buiten de EU kunnen hoge tarieven gelden. Houd het gebruik altijd strikt zakelijk.

Voor sommige risicolanden buiten de EU, zoals China, gelden aparte afspraken voor gebruik en meenemen van CBS-apparatuur. Informeer daar tijdig naar.

4.4 Op vakantie

Als je op vakantie bent, ben je vrij. Het is vaak niet nodig dat je bereikbaar moet zijn. Laat daarom je werkapparatuur thuis.

Is het toch noodzakelijk CBS-devices (bijvoorbeeld de telefoon) mee te nemen, maak daarover dan afspraken met je leidinggevende. Bij reizen buiten de EU gelden vanwege veiligheid en kosten strengere voorwaarden.

4.5 Privégebruik zakelijke ICT-voorzieningen is beperkt toegestaan

Beperkt privégebruik van ICT-voorzieningen is toegestaan. De voorwaarde is dat het je eigen werk en dat van je collega's niet hindert.¹

4.6 Wachtwoorden: maak het anderen niet te gemakkelijk

Leen je account en wachtwoord niet uit en gebruik wachtwoorden die niet makkelijk te raden zijn. Je krijgt toegang tot ICT-voorzieningen op basis van een persoonlijke gebruikersnaam. Je account en wachtwoord zijn van jou en die leen je niet uit. Dit geldt ook voor je toegangspas. Jij bent verantwoordelijk voor wat er met jouw account wordt gedaan.

Veel wachtwoorden? Gebruik een wachtwoordenkuis. Er zijn nog diverse voorzieningen en applicaties met een eigen wachtwoord. Al die wachtwoorden onthouden is moeilijk. CBS heeft **5.1.2.e** als standaard "wachtwoordenkuis". Deze is via TopDesk aan te vragen. Hierin kan je alle wachtwoorden veilig opslaan. Ook kan **5.1.2.e** wachtwoorden voor je bedenken zodat je steeds andere wachtwoorden gebruikt.

5. Het gebruik van e-mail en slack

5.1 CBS-mail is veilig binnen het CBS

E-mail vertrouwelijke informatie alleen naar CBS e-mailadressen. Binnen het CBS kunnen we veilig mailen, omdat we de informatie over een beveiligd netwerk sturen. Buiten het CBS is dat niet het

¹ Tip: stuur je een privé-mailtje of sla je een privé-document op, op het werk? Zet deze bestanden/berichten in een aparte map 'Privé': dan is dit duidelijk voor je collega's en bij een formeel informatieverzoek.



geval. E-mail die over het internet verstuurd wordt, is niet beveiligd tenzij je extra maatregelen neemt. Stuur dus geen vertrouwelijke informatie via het internet.

Is het toch noodzakelijk om vertrouwelijke documenten naar een externe zakelijke partner te e-mailen? Versleutel de documenten dan vooraf met een goed wachtwoord.² Deel het wachtwoord niet per e-mail maar via een ander medium zoals telefonisch. Een alternatief is het delen van het bestand via Secure File Transfer Platform.

Een tikfout in een e-mailadres is zo gemaakt en namen worden in de e-mail aangevuld.³ Let dus op naar wie je e-mail stuurt. Gaat het toch mis en betreft het vertrouwelijke informatie? Probeer de mail in te trekken indien mogelijk. Meld dit als incident/datalek, vraag die persoon de e-mail direct te verwijderen en dat te bevestigen indien intrekken niet gelukt is. En informeer bij je privacycoördinator, de Chief Privacy Officer of de Functionaris Gegevensbescherming of verdere acties nodig zijn.

5.2 Stuur geen vertrouwelijke gegevens naar je privé e-mailadres

E-mail is onderweg tussen de CBS-omgeving en je privé e-mailadres niet beveiligd. Bovendien is privéapparatuur in het algemeen niet veilig genoeg. Stuur dus geen e-mail naar huis, maar maak gebruik van de door het CBS verstrekte middelen (telefoon en laptop) of de thuiswerkvoorziening.⁴

Het is niet werkbaar om in alle mogelijke gevallen aan te geven wat wel en wat niet naar een privé e-mailadres gestuurd mag worden. Hieronder zijn wel enige richtinggevende voorbeelden gegeven.

De volgende bestanden/berichten mogen absoluut niet naar een privé e-mailadres gestuurd worden:

- bestanden met microdata (personen of bedrijven);
- onvoldoende beveiligde statistische tabellen (met reëel onthullingsrisico);
- berichten waarin personeelsvertrouwelijke gegevens van anderen zijn opgenomen, zoals beoordelingen en sollicitatiebrieven;
- CBS-vertrouwelijke informatie, zoals nog niet gepubliceerde (concept)persberichten, inloggegevens en niet-openbare bedrijfsinformatie.

Wat mag in noodzakelijke gevallen wel:

- vergaderverzoeken in webex, teams en dergelijke, die niet goed uitvoerbaar zijn in de CBS-omgeving.

² Aangetekende papieren post is soms een goed alternatief om informatie te versturen. De papieren post is wettelijk beschermd met het briefgeheim. Op schending van het onrechtmatig of onbeveiligd verzenden van vertrouwelijke informatie staan sancties, waaronder boetes en zelfs gevangenisstraffen.

³ Tip: bij het intypen van een e-mailadres wordt de naam automatisch aangevuld. Soms staat hier een oud of verkeerd e-mailadres. Ga achter dat e-mailadres staan en klik op het kruisje: dan komt het foutieve e-mailadres niet meer terug.

⁴ Tip: indien je niet zeker weet of het bestand naar je privé e-mailadres verstuurd mag worden, stel de vraag via Topdesk.



Wat mag altijd wel:

- privéberichten zonder zakelijke inhoud;
- presentaties voor externen (zonder vertrouwelijke gegevens);
- kopieën van eigen personeelsgegevens;
- reisbescheiden voor een dienstreis;
- openbare CBS-bedrijfs- of statistische informatie.

5.3 Slack is een veilige omgeving om met CBS'ers informatie uit te wisselen

Binnen het CBS heeft iedereen toegang tot een afgeschermd Slackomgeving. De CBS Slack omgeving is alleen beschikbaar op een CBS beheerd apparaat. Dit is een veilige plaats om met andere CBS'ers informatie uit te wisselen (en te chatten).

Als je bijvoorbeeld stukken wilt delen of heb je een inhoudelijke vraag over een of meerdere onderzoeken, met uitzondering van statistische data, die je wilt delen met een collega of met je team, maak dan gebruik van Slack als zakelijk communicatiemiddel en geen WhatsApp of andere chatprogramma's.

6. Veilig en correct gebruik van internet

6.1 Blijf weg van riskante websites

Het bezoeken van sommige websites is op het werk of met de door het CBS verstrekte middelen niet toegestaan, ook niet in beperkte mate. Dit betreft bijvoorbeeld pornografische, extremistische, terroristische en goksites. Integriteit is een grondhouding en is een belangrijk onderdeel van de manier waarop je je functie uitoefent. Blijf dus weg bij dergelijke websites.

Sommige websites zijn om andere redenen ongewenst. Op het internet komen ook malafide websites voor, bijvoorbeeld waar je gratis films, muziek en software kan krijgen. Je loopt daar extra risico's op virussen en je kunt auteursrechten schenden.

Het opslaan en verspreiden van dergelijke bestanden binnen het CBS-netwerk of op door het CBS-verstrekte ICT-middelen is niet toegestaan.

6.2 Klik niet zomaar op links

Cybercriminelen vallen met phishing e-mails ook organisaties aan. Ook CBS-mailadressen worden met grote regelmaat benaderd met phishing mails. Het overgrote deel van deze mail wordt tegengehouden door de spamfilters, maar het is niet uit te sluiten dat er zo nu en dan een mail doorheen glipt. Er zijn phishing e-mails die virussen verspreiden en bijvoorbeeld bestanden op slot zetten met losgeld als doel. Klik dus nooit zomaar op linkjes in e-mailtjes. Als je toch denkt dat het een 'echt' bericht is, klik dan niet op de link, maar ga zelf naar de website en log daar in. Of neem zelf rechtstreeks contact op per telefoon of e-mail. Phishing kan grote gevolgen hebben voor de organisatie waarin je werkt. Dagelijks worden organisaties door dergelijke software platgelegd en het herstel kost veel tijd en geld.



Een overzicht van de meest hinderlijke phishing mails van de laatste tijd vind je op [deze](#) pagina.

Via Topdesk meldingsformulier "Poging tot phishing" (via "Ik wil een storing melden", "Werkplek") kunnen phishing en andere hinderlijke en gevaarlijke e-mail berichten gemeld worden. Sla de mail op als een bestand en hang het bestand aan de Topdeskmelding om de verborgen mail headers zichtbaar te maken.

6.3 *Respecteer intellectueel eigendom*

Voor informatie en afbeeldingen die je van het internet of andere media haalt, gelden drie regels:

- pas bronvermelding toe;
- gebruik zoveel mogelijk rechtenvrij materiaal;
- schaf waar nodig betaald materiaal aan.

Op het internet staan veel informatie, filmpjes, muziek en afbeeldingen die voor het werk nuttig zijn. Dit materiaal kan beschermd worden door het auteursrecht. Soms is materiaal rechtenvrij en mag je dat gratis gebruiken met bronvermelding. In zoekmachines zoals Google, kun je je resultaten daarop filteren.

Als je toch beschermd materiaal nodig hebt, moet je het laten aanschaffen.

7. Veilige (privé-)apparatuur

Zakelijk en privé: houd je software en virusscanner actueel en voer updates uit.

Houd zakelijke informatie op zakelijke apparatuur en binnen de zakelijke werkomgeving. Van privé-apparatuur is de veiligheid niet gegarandeerd. Ook is bekend dat deze vaak virussen hebben en andere beveiligingsissues. Zet dus geen documenten via de e-mail of een USB-stick op je privé-apparaat. Maak zo veel mogelijk gebruik van de zakelijke apparatuur (smartphone, laptops, tablet etc) die aan jou verstrekt is door het CBS.

Als je een privé-apparaat gebruikt voor toegang tot de VDI omgeving, zorg te allen tijde ervoor dat alle (security) updates van de aanwezige software geïnstalleerd zijn en zorg ervoor dat de virusscanner up-to-date is. Op een privé-apparaat is het alleen mogelijk om gebruik te maken van CBS Zoom en VDI desktop. Alle andere CBS diensten worden niet aangeboden op je privé apparaat.

Installeer op je telefoon (en tablet) alleen maar apps vanuit de Appstore en Playstore. In de erkende appstores (App Store, Google Play, Windows Store, etc.) staan betrouwbare apps. Apps die van andere plekken komen, kunnen virussen e.d. bevatten. Virussen kunnen documenten op slot zetten waardoor organisaties langdurig niet kunnen werken en het herstel daarvan is kostbaar.



Sommige medewerkers kunnen zelf software op hun laptop installeren. Populaire software kun je overal downloaden en soms krijg je daarbij gevaarlijke extra's. Installeer alleen software die rechtstreeks van de leverancier komt of via een link op de website van de leverancier.

Het internet is zoveel mogelijk vrij toegankelijk. Je kunt dus gebruik maken van allerlei handige gratis diensten. Handig is echter niet altijd veilig(!). Daarnaast kun je zo het eigenaarschap van je gegevens kwijtraken.

Geef je gegevens niet zomaar weg voor een gratis app. Een gratis dienst is nooit echt gratis: de aanbieders van die diensten moeten ook geld verdienen. Soms is dat simpelweg door reclame-inkomsten. Soms handelen ze in je gegevens en heb je daar bij het installeren van de app toestemming voor gegeven. Geef je gegevens niet zomaar weg voor een handige app, maar denk na of het je dat wel waard is.

Als je apparatuur laat repareren, moeten eerst de zakelijke gegevens op het apparaat worden verwijderd. Voor zakelijke apparatuur is dit eenvoudig. Je levert het defecte apparaat in bij de IT-servicebalie en daar wordt dit verder geregeld.

Op privéapparatuur staan, als het goed is, geen zakelijke documenten maar misschien wel contactgegevens. Verwijder zakelijke informatie voorafgaand aan de reparatie. Doe dit ook als je privé-apparatuur verkoopt of weggooit. Lukt het technisch niet meer om deze zakelijke informatie te verwijderen, meld dit dan bij de IT-servicebalie

8. Meld een beveiligingsincident altijd op de geëigende plaats

Fouten maken of je vergissen is menselijk. Je kunt bijvoorbeeld klikken op een verkeerde link in een e-mailbericht, een document achterlaten in het Openbaar Vervoer of je telefoon kan worden gestolen. Fouten maken kan, ervan leren moet. Als er iets misgaat of dreigt mis te gaan, meld je dit in TopDesk en zorg je ervoor dat het incident wordt opgelost (zelf of door een ander). Schaam je hier niet voor, het kan iedereen gebeuren, en wees niet bang voor reprimandes.

Bij diefstal en verlies van mobiele apparatuur moet je dit melden bij de IT-servicedesk. Soms moet je ook aangifte doen. Overleg dit met je leidinggevende.

9. Specifiek: extra voorzichtig met persoonsgegevens

Met persoonsgegevens van personeel of respondenten (incl. indirect via registers) zijn we nog zorgvuldiger dan met interne beleidsstukken en dergelijke.

9.1 Personeelsgegevens

Deel en bespreek niet meer informatie over personen dan nodig voor je werk en voor het werk van de collega. Ook zonder privacywetgeving is het vanzelfsprekend dat je zorgvuldig met



persoonsgegevens omgaat. Je wilt zelf ook graag dat een ander zorgvuldig omgaat met jouw gegevens. Als het voor je werk en van je collega nodig is om persoonsgegevens te delen en daarover te praten, is dat prima. Echter, deel en bespreek niet meer informatie over personen dan nodig voor dat doel. Met trots en plezier praten over je werk is uitstekend, maar pas op welke (persoons)gegevens je daarbij deelt.

9.2 Statistische gegevens

Velen van ons werken voor ons statistisch werk dagelijks met persoonsgegevens, d.w.z. gegevens die direct of indirect te herleiden zijn tot een persoon.

Goed omgaan met persoonsgegevens is cruciaal voor het vertrouwen van de samenleving in het CBS. Hiervoor zijn al enkele voorbeelden genoemd van dingen die niet zijn toegestaan, maar denk hierbij ook aan het opzoeken van personen in bestanden voor eigen doelen of interesses of het doen van analyses die buiten de afgesproken onderzoeksopdracht vallen.⁵

9.3 Advies

Het CBS heeft veel aandacht voor privacy, maar het kan toch voorkomen dat er meer gegevens dan nodig verwerkt worden of dat deze langer dan nodig bewaard blijven. Maak je je hier zorgen over? Bespreek dit dan in je team of vraag het aan de Chief Privacy Officer of de privacycoördinator van jouw hoofddirectie

9.4 Datalekken: meld het als het misgaat

Privacy is essentieel voor het vertrouwen in het CBS. Je moet persoonsgegevens kunnen gebruiken voor je werk, maar anderen moeten er niet zomaar bij kunnen. Door veilig om te gaan met persoonsgegevens bescherm je de privacy van burgers en medewerkers. De clean desk policy, de papiercontainer, nadenken wat je bespreekt in de openbare ruimte etc. dragen ook bij aan privacybescherming.

Een datalek ontstaat als de verkeerde personen toegang, (kunnen) krijgen tot persoonsgegevens en wanneer persoonsgegevens vernietigd worden zonder dat dit de bedoeling is.⁶

Meld altijd wanneer persoonsgegevens bij de verkeerde persoon terecht komen. Doe dit ook als het risico voor de betrokkenen beperkt is. Ook als je heel zorgvuldig werkt, kun je toch een datalek veroorzaken. Dit kan ook buiten je schuld zijn als bijvoorbeeld post zoekraakt met daarin persoonsgegevens. Door consequent te melden, zien we ook waar ruimte is voor verbetering in proces, systeem en instructie. In de verdere afhandeling wordt ervoor gezorgd dat impactvolle datalekken gemeld worden bij de Autoriteit Persoonsgegevens. Het is belangrijk dat je een potentieel datalek direct meldt zodat we deze tijdig kunnen melden bij de Autoriteit Persoonsgegevens. Ook is op die manier de administratie op orde bij eventuele vragen van de Autoriteit Persoonsgegevens.

⁵ Dit geldt uiteraard ook voor gegevens over bedrijven en instellingen.

⁶ Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie, zonder dat dit de bedoeling is van deze organisatie. Aan een datalek ligt altijd een beveiligingsincident ten grondslag.



Een datalek kun je bij het CBS melden bij de Functionaris Gegevensbescherming via Topdesk.⁷

10. Loggen en monitoren: jouw privacy op het werk

Op het werk heb je ook recht op privacy, bijvoorbeeld met betrekking tot je e-mail en je home directory/persoonlijke schijf. Sommige handelingen met ICT worden digitaal gelogd en gemonitord. Het beleid hierover is vastgelegd in notities en door de OR goedgekeurd.⁸ Het voornaamste doel hiervan is ICT-beheer waaronder het oplossen van verstoringen en het detecteren van dreigingen. Verder kunnen loggegevens worden ingezien met heel goede redenen en via vastgestelde procedures, zoals bijvoorbeeld voor rechtsgangverzoeken of integriteitsonderzoek.

11. Sancties

Het goed opvolgen van bovenstaande gedragsregels raakt tot de kernwaarden van het CBS. Burgers moeten erop kunnen vertrouwen dat hun gegevens in veilige handen zijn. Dat geldt zowel voor de technische voorzieningen als voor het gedrag van de CBS'er die met deze data werkt.

Het kan altijd gebeuren dat er zonder opzet iets fout gaat. Als je dat (tijdig) meldt, dan kunnen we dat oplossen en ervan leren voor een volgende keer.

Als je je bewust niet aan de gedragsregels houdt, kan dat voor jouw leidinggevende aanleiding zijn om dat te bespreken. Dit kan leiden tot nadere afspraken, een training, en bij ernstiger situaties tot een aantekening in je personeelsdossier en integriteitsonderzoek. Dit is iets tussen jou en je leidinggevende en loopt via de daarvoor vastgestelde procedures.

Om een richtlijn te geven op welke manier met welke gedragingen (onder andere uit deze gedragsregeling) wordt omgegaan, hanteert het CBS een sanctiebeleid. Het sanctiebeleid is opgenomen in het personeelsreglement.

12. Gerelateerde onderwerpen/documenten

De volgende documenten beschrijven de invulling bij het CBS van een aantal gerelateerde onderwerpen:

⁷ Dat kan op dit moment via Topdesk, tegel (IT) Security / Beveiliging, en vervolgens de knop Melden van een datalek. In de toekomst komt er direct in het hoofdmenu van Topdesk een tegel voor het melden van een datalek.

⁸ Op dit moment is de notitie over logging gereed en goedgekeurd. Op basis van voorliggende notitie over gedrag zal het beleid rond monitoring worden uitgewerkt.



- [Gedragscode Integriteit CBS](#): Dit omvat afspraken op het gebied van integriteit en helpt bij het maken beslissingen op dit gebied.⁹
- Notities uit DIOR over Communicatiemiddelen: hierin staat hoe je integer en professioneel gebruik maakt van online voorzieningen waaronder social media.
[Moet nog definitief gemaakt worden]

Bronvermelding

Deze notitie is in belangrijke mate ontleend aan de “Gedagsregeling voor de digitale werkomgeving” d.d. september 2021 van het Rijksprogramma Duurzaam Digitale Informatiehuishouding (RDDI) en aangepast en aangevuld voor de specifieke situatie bij het CBS.

⁹ Personeelsreglement, hoofdstuk 5.