

Gedragcode

Regeling: Goed overweg met informatie

ProRail staat altijd volop in de publieke belangstelling. We krijgen speciale aandacht van controle organen zoals de Autoriteit Persoonsbescherming (AP) en de Autoriteit Consument en Markt (ACM). Voor de reputatie en het succesvol functioneren van ProRail is zorgvuldig omgaan met (vertrouwelijke) informatie van groot belang. Denk aan gegevens over de bedrijfsvoering en het beleid en privacygevoelige gegevens over medewerkers, leveranciers of klanten. Als medewerker van ProRail krijg je elke dag veel en diverse soorten informatie onder ogen. Variërend van telefoonnummers tot rapportages en van financiële gegevens tot notulen. Via e-mail, gesprekken, Focus, SharePoint en in overleggen word je voortdurend geconfronteerd met informatie. Die informatie heb je gewoon nodig om je werk te kunnen doen. Daarmee draag je direct of indirect bij aan onze primaire taak: treinverkeer mogelijk maken.

Weet jij alle informatie over informatiebeheer en informatieveiligheid te vinden, weet je überhaupt van het bestaan af? In dit reglement is deze informatie voor je samengebracht.

Waarom hebben wij deze regeling “Goed overweg met informatie” nodig?

ProRail heeft alle regels over hoe om te gaan met (vertrouwelijke) informatie handig in een reglement bij elkaar gezet zodat jij als medewerker weet op welke wijze je met (vertrouwelijke) informatie moet omgaan. Iedere ProRail-medewerker is verantwoordelijk voor de veiligheid van onze informatie. Jij bent er zelf voor verantwoordelijk dat informatie en systemen op een verantwoorde en veilige manier worden gebruikt. Daarnaast is het jouw plicht als medewerker om anderen (indien nodig) erop te wijzen juist te handelen.

De hoeveelheid informatie en het aantal kanalen waarin informatie tot ons komt, blijven toenemen. We kunnen steeds makkelijker, sneller en vanaf verschillende locaties toegang tot deze informatie krijgen. De keerzijde hiervan is dat informatie soms versnipperd raakt en dat daarmee

onoverzichtelijk wordt welke informatie op welke manier toegankelijk is en voor wie. Het plaatsen van een vacature is uiteraard transparant, maar jouw personeelsdossier of een onderzoeksrapport over een gezamenlijk project zijn bij uitstek vertrouwelijke kwesties waarvan je niet wilt dat dit toegankelijk is voor iedereen.

Meer informatie over hoe je op een verantwoorde en bewuste wijze omgaat met informatie vind je in ons [Informatiebeveiligingsbeleid](#).

Informatiebeveiliging is het beschermen van informatie tegen een steeds breder wordend spectrum van bedreigingen zoals cyber-aanvallen, hacks of phishing mails die de bedrijfscontinuïteit in gevaar kunnen brengen of ons imago kan schaden. Uitgangspunt voor informatiebeveiliging blijft altijd dat de balans bewaard blijft tussen de vrijheid die jij als medewerker hebt om informatie te delen en de manier waarop onze bedrijfsinformatie wordt beveiligd.

Duidelijke werkafspraken

Het is lastig om algemeen geldende regels voor de omgang met informatie vast te leggen voor de gehele organisatie. Dit wordt al snel zo algemeen dat jij als medewerker geen handvatten meer hebt. Beter is het om met je team of afdeling duidelijke werkafspraken te maken waar je jullie documenten opslaat, in welke applicaties en met welke kenmerken. Het is belangrijk dat we altijd en overal actuele en geldende afspraken en documenten kunnen terugvinden. Binnen ProRail gelden daarom verplichte documenteisen. Alle documenten moeten zijn voorzien van onderwerp, eigenaar, kenmerk en status. Deze eisen kunnen naar wens aangevuld worden met bijvoorbeeld datum, versie of geldigheid. Over het algemeen geldt dat SharePoint gebruikt kan worden voor het opslaan van gezamenlijke documenten en OneDrive voor persoonlijke documenten. Voor vertrouwelijke stukken kun je een vertrouwelijke SharePoint site of vertrouwelijke documentbibliotheek aanvragen. Het kan natuurlijk zijn dat je voor jouw werkzaamheden een specifieke applicatie moet gebruiken zoals SAP of VISI.

Gedragscode

Regeling: Goed overweg met informatie

Duidelijke werkafspraken zorgen ervoor dat je de documenten van jezelf en van je naaste collega's snel kunt terugvinden. Ook hoeft je geen omwegen te gebruiken wanneer je documenten wilt delen, zodat de juiste bedrijfsinformatie alleen terechtkomt bij de mensen voor wie het bedoeld is.

Voor meer informatie en voor hulp bij SharePoint kun je terecht op [PROSA](#).

Verschillende soorten informatie

Als medewerker moet je je bewust zijn van vertrouwelijke en/of geheime informatie en wanneer hier sprake van is. De informatie die wij binnen ProRail gebruiken is in te delen in vier klassen: Openbaar (0), Intern (1), Vertrouwelijk (2) en Geheim (3). Hoe je omgaat met informatie van ProRail is afhankelijk van het belang ervan voor ProRail, de medewerkers en de stakeholders, maar ook van de wet- en regelgeving waaraan wij ons moeten houden. Belangrijkere informatie vraagt om strakkere regels. Hierbij moet je ook denken aan informatie die niet op papier staat maar bijvoorbeeld in telefoongesprekken aan de orde komt.

Classificaties

Het volgende schema helpt je om de mate van vertrouwelijkheid van informatie te herkennen. Niet alleen het belang van ProRail, maar ook wet- en regelgeving spelen hierbij een rol. Gebruik deze classificaties ook als je een document opslaat in SharePoint, zodat in één oogopslag duidelijk wordt wat de status van een document is.

Niveau	Naam	Beschrijving	Toegang
0	Openbaar	Informatie is openbaar, bestemd voor iedereen en vrij toegankelijk. Bijvoorbeeld publieke informatie op een website, op folders, in brochures.	Iedereen, in- en extern
1	Intern	Informatie is bedoeld voor Intern gebruik. Openbaar worden van gegevens leidt tot weinig of geen schade. Bijvoorbeeld: Algemene informatie over klanten, breed toegankelijke informatie op Intranet, beleidsdocumenten enz. Uitgangspunt is dat je er rekening mee moet houden dat iets wat intern verspreid wordt, altijd extern terecht kan komen.	Alle ProRailers
2	Vertrouwelijk	ProRail kan substantiële schade lijden als informatie toegankelijk is voor ongeautoriseerde personen. Informatie is alleen toegankelijk voor personen die hier vanuit hun functie toegang toe moeten hebben (need to know). Hieronder vallen ook persoonsgegevens.	Met name kantoormedewerkers of door ProRail ingehuurd krachten die een geheimhoudingsverklaring hebben ondertekend
3	Geheim	ProRail kan grote schade lijden als informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag uitsluitend toegankelijk zijn voor een zeer selecte groep van personen. Bijvoorbeeld: Strategische plannen, informatie over toekomstige investeringen, samenwerkingsverbanden. Persoonlijke (medische) informatie, inhoudelijke informatie over zeer ernstige beveiligingsincidenten, etc.	Voor bedrijfsinformatie met name het hoger management van ProRail en beleidsmedewerkers. Arboartsen voor medische gegevens

Meer uitleg over classificaties vind je in ons [Handboek voor Informatiebeveiliging](#).

Gedragcode

Regeling: Goed overweg met informatie

Gezond verstand

De auteur van een document bepaalt zelf de classificatie. Daarvoor gebruikt hij bovenstaande tabel en hij maakt een afweging op basis van gezond verstand. Dit betekent dat je nadenkt over wat het gevolg zou zijn als de informatie uitlekt of in verkeerde handen komt. Stel jezelf de vraag of je het erg zou vinden als de informatie algemeen bekend zou worden of als het bekend zou worden dat dat is gebeurd door jouw toedoen. Twijfel je over de classificatie van je informatie? Bespreek het dan in je team en met je leidinggevende. De Information Security Officer (ISO) kan je hier ook bij helpen. In bijlage 1 bij dit reglement tref je een overzicht aan met voorbeelden van classificatie.

Zorgvuldig omgaan met bedrijfsinformatie.

Niet alle informatie is voor iedereen bestemd. Het is dan ook belangrijk om je bewust te zijn van je omgeving als je vertrouwelijke of geheime informatie deelt met anderen. Dat geldt niet alleen voor informatie op schrift (waaronder ook bedoeld e-mail), maar ook informatie die ter sprake komt in een overleg of telefoongesprek. Het is je plicht als ProRailer om bij het uitwisselen van vertrouwelijke en geheime informatie te voorkomen dat anderen deze kunnen horen en inzien.

Zo is het niet handig contractbesprekingen te voeren in de trein of op sociale media te zetten dat je net een vervelend (beoordelings)gesprek hebt gehad met je leidinggevende. Ook is het belangrijk om geen vertrouwelijke stukken op je bureau te laten liggen.

De informatie die je nodig hebt om je werk te kunnen doen, is en blijft van ProRail. Vanzelfsprekend betekent dat dat je die informatie ook niet mee mag nemen als je niet meer bij ProRail werkt.

Tips bij het omgaan met informatie:

- Zorg ervoor dat vertrouwelijke informatie ook vertrouwelijk blijft. Dit geldt zowel voor informatie op papier, als voor elektronisch vastgelegde informatie.
- Verspreid, communiceer of publiceer geen vertrouwelijke of geheime informatie zonder toestemming van de leidinggevende.
- Wees er alert op dat anderen onbedoeld mee kunnen luisteren als het over het werk gaat, bijvoorbeeld in de trein. Dat is niet de bedoeling.
- Laat bedrijfsgevoelige of vertrouwelijke informatie nooit onbeheerd achter op je bureau of op een andere plek. Dit geldt niet alleen voor schriftelijke informatie, maar

ook voor informatie waarmee je op je computer aan het werken bent; vergrendel dus altijd je computer als je je werkplek verlaat.

- Maak verstandig gebruik van middelen als versnipperaars, kasten, archieven, wachtwoorden, back-up diensten en internet en zorg dat sleutels en wachtwoorden opgeborgen zijn.
- Wees voorzichtig met digitale uitwisseling en verzending van informatie en het onnodig vervoeren van vertrouwelijke stukken.

In bijlage 2 van dit reglement kun je opzoeken welke regels gelden voor welke informatieklassen.

Eigendommen en middelen van ProRail

Middelen van ProRail zoals laptops, telefoons en dergelijke zijn er voor het uitvoeren van het werk. Beperkt privé-gebruik daarvan is toegestaan, maar het eigendom blijft altijd bij ProRail.

Als ProRailer mag je op je laptop, smartphone of een ander ProRail apparaat geen informatie raadplegen, verspreiden of uitwisselen als daardoor bedrijfsvertrouwelijke informatie uitlekt of je daarmee de privacy van personen schendt. Een ProRail apparaat is beschikbaar voor privédoeleinden zolang je daarmee geen ProRail belangen schaadt. Bij privé apparaten die je voor bedrijfsdoeleinden gebruikt, dien je ervoor te zorgen dat het op een vergelijkbare wijze is beveiligd als een ProRail apparaat. Voor vertrouwelijke en geheime informatie gelden strengere regels.

In het Huisreglement van ProRail zijn de regels over de middelen van ProRail uitgebreid te vinden. Wil je graag meer te weten komen over dit onderwerp klik dan [hier](#).

Gedragcode

Regeling: Goed overweg met informatie

Juiste omgang met ICT middelen

ProRail stelt een variëteit aan hard- en software aan de medewerkers ter beschikking. Van smartphone tot juridisch documentatie systeem en van laptop tot voorziening om ook buiten kantoor al jouw relevante werk-informatie te kunnen benaderen via de cloud. Deze functionaliteit vraagt om sterk toegespitste afspraken voor het gebruik in relatie tot informatieveiligheid. Met de eerder besproken classificaties in documenten is daar al een hele duidelijke richtlijn aan meegegeven.

Hieronder wat praktische tips om ervoor te zorgen dat je veilig gebruik maakt van de ICT middelen die ProRail aanbiedt. Voor uitgebreide toelichting kun je ons [Handboek voor Informatiebeveiliging](#) raadplegen.

Digitale informatie

- Computers, smartphones, USB-sticks en vergelijkbare informatiedragers moeten beveiligd zijn met een sterk wachtwoord, schermbeveiliging en worden nooit onbeheerd achtergelaten.
- Toegangscodes en wachtwoorden zijn persoonlijk en vertrouwelijk en dienen daarom versleuteld op computers/telefoons te worden opgeslagen. Doe dat dus niet onversleuteld in een Word of Excel bestand, en al helemaal niet op een memoblaadje bewaard bij je computer. Het is ook niet toegestaan om toegangscodes en wachtwoorden te helpen achterhalen of te verstrekken aan onbevoegden.

Gebruik bedrijfsnetwerk, internet en e-mail

- Het bedrijfsnetwerk mag niet worden gebruikt om informatie van intimiderende, illegale, erotische, pornografische, racistische of kwetsende aard te downloaden van- of te bekijken op internet.
- Spam versturen of het internetverkeer op een andere manier verstoren of blokkeren, is niet toegestaan.
- Een medewerker die ongewenste informatie ontvangt, wist de gegevens en laat de afzender indien mogelijk weten dat hij dergelijke informatie niet via bedrijfs-faciliteiten wenst te ontvangen. Als de informatie blijft komen, informeert de medewerker de systeem-beheerder (7100/ServiceDesk ProRail).
- Als een medewerker vermoedt dat zijn internet-faciliteiten worden misbruikt door anderen, dan meldt hij dit aan zijn leidinggevende.
- Informatie die wordt verzonden vanaf een e-mailadres van ProRail, wordt met het bedrijf geassocieerd.

Verzend daarom geen, niet werkgerelateerde, e-mails op persoonlijke titel vanaf een ProRail e-mail adres.

- Het gebruik van het ProRail e-mailadres als login op een niet-zakelijke toepassing op Internet is niet toegestaan (zoals: fora, datingsites, webwinkels enzovoort). Ook niet als hier iets gekocht wordt voor een collega bij verjaardag of geboorte.
- Incidenteel internet gebruiken voor privédoeleinden mag, als het met mate gebeurt en het geen negatieve invloed heeft op de werkzaamheden en de beschikbaarheid van Internet voor andere werknemers (denk aan het streamen van videobeelden tijdens sportevenementen als WK voetbal, Olympische Spelen en dergelijke).
- Het is niet toegestaan om via de internetfaciliteiten van ProRail privéaankopen te doen.
- Gegevens die onder het auteursrecht vallen, mogen niet ongeautoriseerd worden gebruikt of gedownload (denk aan films, muziek, illegaal verkregen betaalde content en dergelijke).

Een handeling die onschuldig lijkt, is het online kopen van privéspullen met bijvoorbeeld je e-mail-adres (en erger nog je wachtwoord) van ProRail. Deze gegevens worden opgeslagen op de website van de verkoper. Deze website is veelal minder goed beveiligd en daarom vatbaarder voor hackaanvallen. Dit kan tot gevolg hebben dat informatie van ProRail in handen van kwaadwillenden terecht komt die vervolgens jouw gegevens oneigenlijk kunnen gebruiken om zo aan vertrouwelijke ProRail informatie te komen.

Gebruik hard- en software ProRail en privé

Ongeacht of een mobiel apparaat eigendom is van ProRail of van de medewerker, in toenemende mate vloeien privé- en zakelijk gebruik in elkaar over. Hierbij ontstaat het risico dat vertrouwelijke bedrijfsinformatie terecht komt in een omgeving die niet beveiligd is. Voorbeelden zijn lokale opslagruimten (SD-kaart), Cloud storage diensten en sociale media. Daarom is het noodzakelijk privé- en zakelijke gegevens zoveel mogelijk van elkaar te scheiden. Dit kan in de mobiele applicatie door gegevens versleuteld op te slaan en alleen uit te wisselen met betrouwbare systemen.

Gedragcode

Regeling: Goed overweg met informatie

Ten slotte is het toegestaan om bijvoorbeeld je werk-email op een privé apparaat te ontvangen mits deze wordt beschermd door een toegangscode of wachtwoord. Voor het verzenden van vertrouwelijke en geheime informatie geldt dat deze niet naar een privé apparaat (door)gestuurd mogen worden.

Uitgebreidere informatie over de dunne scheidslijn tussen privé en ProRail apparaten of het gebruik daarvan, is te lezen in het [Beveiligingsbeleid Mobile](#) (Devices & Apps).

Toegang tot en werken op kantoren

In alle ProRail panden is de toegang beveiligd. Iedereen is verplicht de pas zichtbaar te dragen. Iedere ProRail medewerker heeft een toegangspas, we kennen een aanmeldprocedure voor bezoekers en de clear desk policy. Alles staat of valt echter met de uitvoering daarvan en daar ben jij als medewerker de hoofdrolspeler in.

Toegangspas

Iedere medewerker van ProRail (incl. inhuur op naam en stagiairs) ontvangt bij indienstreding een ProRailpas die toegang geeft tot alle algemene ruimten van de bemenste ProRail locaties. Toegang tot een ruimte is alleen toegestaan zolang daar een functionele reden voor is. Het hebben van een werkende pas op een deur van een ruimte is geen reden om je in een ruimte te bevinden waar je niet hoort te zijn. Het aanspreken op misbruik is van groot belang en is een gezamenlijke verantwoordelijkheid van alle ProRailers. Indien je jouw pas bent verloren of als de pas is gestolen dan moet je de pas z.s.m. zelf laten blokkeren en een nieuwe aan vragen. Dit kan 24/7 via 'mijn beheer' in de ProRail Aanmeldservice Toegang (PAT). Problemen met je toegangspas (verlies, diefstal of defect)? Meer informatie vind je op: [Focus / Hoe regel ik / Toegang](#).

Bezoekers

Voorwaarde voor toegang tot de gebouwen van ProRail is dat de ProRail-medewerker de bezoeker aanmeldt en dat hij/zij zich bij aankomst legitimeert. De medewerker is verplicht de bezoeker te begeleiden door het gebouw. Als een bezoeker niet is aangemeld, dan wordt geen toegang verleend. De bezoeker zal op de hoogte worden gesteld dat hij contact dient op te nemen met zijn contactpersoon.

Een bezoeker aanmelden? Meer informatie vind je op: [Focus / Hoe regel ik / Toegang](#)

Clear desk

Het clear desk-beleid is er niet alleen om het flexibel werken te bevorderen, het dient ook een informatiebeleidsdoel. Zo is het laten liggen van (vertrouwelijke of geheime) stukken op je bureau zeer onwenselijk. Daarnaast vormt het ook een risico omdat er een kans op lekken bestaat van geheime en vertrouwelijke informatie. Dit geldt vooral in combinatie met derden die fysieke toegang hebben tot een locatie/gebouw. Zorg er voor dat vertrouwelijke of geheime stukken altijd in een afgesloten kast of in je persoonlijke locker opgeborgen zijn, ook als je wegloopt om bijvoorbeeld koffie te halen.

Denk er ook aan om je laptop te vergrendelen als je even van je werkplek loopt. Dat kan heel eenvoudig door de Windows -toets ingedrukt te houden samen met de letter L. En zorg er verder voor dat de laptop met behulp van een laptopslot vast zit aan je bureau zodat hij niet eenvoudig kan worden meegenomen.

In ons [Huisreglement](#) vind je uitgebreide informatie over ons clear desk beleid.

Melden als er iets misgaat

Tot je schrik merk je dat, ondanks je goede bedoelingen, er mogelijk informatie in handen van derden is gekomen. Ook hiervoor is beleid ontwikkeld.

Denk hierbij aan het verliezen van je toegangspas, maar ook de vermissing of diefstal van je ProRail laptop of telefoon moet je altijd melden. Het melden van mogelijk lekken van informatie helpt ons de beveiliging te verbeteren en in sommige gevallen zijn wij verplicht dit te melden bij een toezichthoudende instantie.

Vermissing binnen ProRail

Iedere vermissing / diefstal van eigendommen meld je via het Self Service Portal. Kijk voor meer informatie bij het onderwerp 'Diefstal' op: [Focus / Hoe regel ik](#). Gaat het om ProRail-eigendommen, dan registreert FaZ de melding. Bij vermissing of diefstal binnen ProRail locaties wordt door FaZ of ICT zelf de afweging gemaakt of

Gedragcode

Regeling: Goed overweg met informatie

aangifte noodzakelijk is. ProRail is alleen verantwoordelijk voor vermissing van ProRail-eigendommen op ProRail-locaties.

Vermissing van privé-eigendommen blijft altijd de verantwoordelijkheid van de eigenaar. Als het om een SIM-kaart en/of tablet gaat, neem je contact op met ICT via 7100, zodat direct actie ondernomen kan worden voor wissen en/of blokkeren. Daarna meld je de vermissing ook op het [Self Service Portal](#). Bij diefstal daarvan doe je zelf aangifte bij de politie. FaZ controleert na je melding de gevonden voorwerpen en geeft je een terugkoppeling. Registreer je vermissing bij FaZ, zodat we eventuele patronen kunnen vaststellen en daarop anticiperen.

Vermissing buiten ProRail

Bij vermissing van ProRail-eigendommen buiten ProRail-locaties (bijvoorbeeld bij verlies onderweg of diefstal uit de woning/auto) doe je zelf aangifte van de vermissing bij de politie. Verder volg je dezelfde stappen als hierboven genoemd onder het kopje 'Vermissing binnen ProRail'.

Voor meer informatie verwijzen wij je naar de [procedure over vermissing en diefstal](#).

Voorkom diefstal – wees alert

Een groot deel van de diefstallen of vermissingen kan voorkomen worden door waardevolle zaken goed op te bergen. Geef dieven geen kans. Voor het veilig opbergen van zakelijke en persoonlijke eigendommen is het belangrijk dat je beschikt over een af te sluiten kast/locker. Facilitaire Zaken faciliteert deze kast/locker. Als je verdachte personen in je werkomgeving ziet, meld dit dan onmiddellijk bij de receptie. Ben je werkzaam op een VL-post, dan kun je verdachte personen melden bij de teamleider van de seinzaal.

Meldpunt datalekken

ProRail is verplicht voorvallen die zich voordoen, zoals hiervoor beschreven, te melden bij het meldpunt datalekken.

Een uitgebreide beschrijving hierover kan je terugvinden in onze [procedure datalekken](#).

Onderzoek & sancties

Evenals de Gedragcode is ook dit reglement niet vrijblijvend. Het zijn beleidsregels die betrekking hebben op professionaliteit binnen onze organisatie. Overtreding van de regels en afspraken uit dit reglement wordt door ProRail gesanctioneerd. Zie ook de [Regeling Sanctionering](#).