



Hoe kies ik het juiste vertrouwelijkheidsniveau?

Als je bij Rijkswaterstaat werkt, dan markeer je het vertrouwelijkheidsniveau van alle documenten, e-mails en andere informatie die je opstelt. Dit helpt iedereen in de organisatie om zorgvuldig met vertrouwelijke gegevens om te gaan. In dit schema zie je welke niveaus we hanteren, bij welke informatie het niveau past en hoe je ermee omgaat. Kijk voor meer informatie op intranet bij 'Ondersteuning'.

0. RWS INFORMATIE

Wat valt onder RWS INFORMATIE?

Er is geen probleem als deze informatie onbedoeld bekend wordt binnen Rijkswaterstaat of partijen die we contracteren. Extern publiceer je de informatie alleen via de formele kanalen.

Voorbeelden:

- interne brochure;
- een instructiedocument over het omgaan met bedrijfsmiddelen;
- e-mails over opleidingen;
- RWS-intranetberichten voor medewerkers.

Hoe ga je ermee om?

- Deze informatie mag je bewerken, versturen en bespreken met alle communicatiemiddelen.
- Bijvoorbeeld ook via WhatsApp of een privételefoon.
- Delen met collega's en externen is toegestaan.
- Opslag mag op openbare schijf of in het postvakje of in open kasten.

1. RWS BEDRIJFS- VERTROUWELIJK

Wat valt onder RWS

BEDRIJFSVERTROUWELIJK?

Als RWS BEDRIJFSVERTROUWELIJKE informatie onbedoeld bekend wordt binnen of buiten RWS, dan kan dat leiden tot lokaal protest en negatief effect op verhoudingen, of leidt tot financiële schade voor RWS (< 1 miljoen euro), of leidt tot lokale negatieve publiciteit en imagoschade.

Voorbeelden:

- een rapport over achterstallig onderhoud;
- beschrijving van netwerkarchitectuur waardoor deze kwetsbaarder wordt;
- financiële overzichten op hoofdlijnen;
- offerteaanvragen.

Hoe ga je ermee om?

- Deze informatie mag je bewerken, versturen en bespreken met communicatiemiddelen van Rijkswaterstaat.
- De informatie mag ook naar leveranciers, mits zij een geheimhoudingsverklaring hebben.
- Deze informatie verspreid je alleen binnen je project of afdeling, op basis van noodzaak.
- De informatie mag alleen te benaderen zijn door bevoegden.

2. DEPARTEMENTAAL VERTROUWELIJK

Wat valt onder DEPARTEMENTAAL VERTROUWELIJK?

Uitlekken van deze informatie kan leiden tot verantwoording van bewindspersoon naar de Tweede Kamer, of leidt tot ernstige financiële schade voor RWS (>1 miljoen euro), of leidt tot Rijksbrede - en landelijke negatieve publiciteit en imagoschade.

Voorbeelden:

- afstemming interdepartementale bestuursstukken;
- concurrentiegevoelige documenten van grote aanbestedingen;
- cruciale beveiligingsinformatie over sluizen en andere objecten die kunnen leiden tot misbruik of sabotage.

Hoe ga je ermee om?

- Delen per e-mail en opslag gaat met versleuteling met een sterk wachtwoord.
- DEPARTEMENTAAL VERTROUWELIJKE informatie mag alleen worden gedeeld met leveranciers als die een verklaring omtrent gedrag hebben.
- Fysiek versturen mag alleen volgens de zogenoemde postinstructie (onder andere: altijd dubbele enveloppe, binnenste is DepV gemarkeerd).
- DEPARTEMENTAAL VERTROUWELIJK moet officieel worden vastgesteld door een lijnmanager. Na 5 jaar moet de lijnmanager heroverwegen of de informatie nog echt DEPARTEMENTAAL VERTROUWELIJK is.



Bevat het document persoonsgegevens?

Als een document ook persoonsgegevens bevat, dan is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Je kiest dan 1 van de 2 niveaus voor vertrouwelijkheid van de persoonsgegevens. Als in een document of mail alleen zakelijke contactgegevens voorkomen, dan hoef je de informatie niet te markeren als persoonsvertrouwelijk.

1. PERSOONSVERTROUWELIJK 2. PERSOONSgegevens ZEER VERTROUWELIJK

Als PERSOONSVERTROUWELIJKE gegevens oneigenlijk gebruikt worden, dan kan dat voor betrokken personen ongewenste gevolgen hebben, bijvoorbeeld onnodig aangesproken worden omdat men weet dat je solliciteert.

Voorbeelden:

- sollicitatiebrieven;
- personeelsadministratie;
- salarisadministratie.

Hoe ga je ermee om?

Met PERSOONSVERTROUWELIJKE gegevens ga je hetzelfde om als met RWS BEDRIJFS-VERTROUWELIJKE gegevens.

Als PERSOONSgegevens ZEER VERTROUWELIJKE gegevens uitlekken, dan heeft dat mogelijk ernstige gevolgen voor personen, bijvoorbeeld identiteitsfraude, misbruik door verzekeringen, uitsluiting van bepaalde groepen e.d.

Voorbeelden:

- politieke opvattingen;
- religieuze of levensbeschouwelijke overtuigingen;
- lidmaatschap van een vakbond;
- genetische gegevens;
- biometrische gegevens met het oog op de unieke identificatie van een persoon;
- gezondheid;
- seksueel gedrag of seksuele gerichtheid
- inloggegevens van bv IT diensten, bank, overheid,...;
- identiteitsgegevens zoals BSN, ID kaart, paspoort.

Hoe ga je ermee om?

Met PERSOONSgegevens ZEER VERTROUWELIJK ga je hetzelfde om als DEPARTEMENTAAL VERTROUWELIJK.