RICHTLIJN **'OMGAAN MET INFORMATIE'**

1. Algemeen

Ordina staat voor zorgvuldig en betrouwbaar. Dat is ook de manier waarop Ordina met informatie omgaat. Wij beschermen informatie, of het nu gaat om informatie van Ordina zelf of om informatie die door klanten, medewerkers, leveranciers of partners aan Ordina wordt toevertrouwd. Wij houden ons aan wettelijke en contractuele verplichtingen tot bescherming en geheimhouding van informatie en aan de relevante interne richtlijnen. De richtlijn 'Omgaan met informatie' is zo'n interne richtlijn.

Deze richtlijn 'Omgaan met informatie' gaat specifiek in op het vertrouwelijkheidsaspect van informatie, oftewel over de vraag met wie je informatie mag delen en hoe je ervoor zorgt dat informatie alleen terecht komt bij personen die er recht op hebben. Het onvoldoende beschermen van informatie of het delen van informatie met niet-geautoriseerde personen kan grote gevolgen hebben. Het kan leiden tot schade, hoge boetes én aantasting van de goede naam van Ordina.

In hoofdstuk 2 is summier beschreven welke soorten informatie Ordina onderscheidt (classificatie). Hoofdstuk 3 gaat over beschermingsmaatregelen voor de verschillende soorten informatie. Hoofdstuk 4 gaat in op de vraag met wie je welke informatie mag delen.
Een aantal specifieke situaties – bijvoorbeeld als je gedetacheerd bent – komt aan de orde in hoofdstuk 5. Tot slot, in hoofdstuk 6 lees je bij wie je terecht kunt in geval van vragen.

2. Soorten informatie

Binnen Ordina maken we onderscheid tussen drie soorten informatie: ongevoelige, gevoelige en kritieke informatie. Deze drie soorten informatie noemen we classificaties. Hoe gevoeliger de informatie is, hoe kleiner de groep personen met wie je de informatie kunt delen, en des te groter de noodzaak om informatie te beschermen. Ook hangt het van het classificatieniveau af of je informatie al dan niet moet labelen. Zie het hoofdstuk Classificatie in het Informatiebeveiligingsbeleid Ordina.

3. Gedragsregels voor het beschermen van informatie

Informatie wordt binnen Ordina op velerlei manieren beschermd. Zo zijn er technische en organisatorische waarborgen genomen om informatie te beschermen, denk aan firewalls, toegangspassen en screening. Deze waarborgen vind je terug op Connect (beleid/beveiliging).

Bovendien gelden bepaalde gedragsregels voor het beschermen van informatie. Over die gedragsregels gaan de paragrafen 3.1 en 3.2.

3.1 Beschermen van Ordina informatie

Neem steeds de volgende basisregels in acht voor het beschermen van informatie (van ongevoelig tot kritiek).

- clean-desk: laat geen belangrijke informatie (papier/usb) onbeheerd op je werkplek achter;
- clear-screen: vergrendel je computer als je je werkplek verlaat;
- voorkom dat veel data op je persoonlijke computer/ laptop staan. Maak gebruik van de mogelijkheden die Ordina biedt, zoals werken met Scope, workspaces, web applicaties, Lync e.d.
- vergrendel mobiele apparaten fysiek (bijvoorbeeld met een laptop slot;
- gebruik alleen de USB harddisk om de data van je Ordina laptop veilig te stellen; gebruik deze niet voor andere doeleinden;
- zorg er bij gebruik van een eigen device (BYOD) voor dat deze aan dezelfde eisen voldoet als de Ordina devices. Zie hiervoor de richtlijn mobiele apparatuur en gegevensdragers (of vraag advies aan de afdeling Informatie Management);
- meld in geval van verlies of diefstal van een mobiel apparaat dit zo spoedig mogelijk aan de je leidinggevende en aan de Security Officer.

Voor gevoelige informatie van Ordina gelden de volgende aanvullende maatregelen

- ga zorgvuldig om met de autorisatie voor toegang tot gevoelige gegevens, zie de richtlijnen Autorisaties;
- zorg dat gevoelige (geprinte) informatie veilig wordt opgeborgen, zowel thuis als op kantoor, minimaal in een afgesloten kast;
- zorg dat gevoelige (geprinte) informatie, bij weggooien, alleen in de afgesloten papierbak terecht komt.

Voor kritieke informatie van Ordina gelden behalve de basisregels en aanvullende maatregelen ook de volgende regels:

- vermijd waar mogelijk het opslaan van kritieke informatie op mobile devices; zorg dat kritieke informatie zich in elk geval uitsluitend op een mobile device bevindt als de encryptie (gegevenscodering) aan de meest recente Ordina data encryption standards voldoet;
- vermijd bij het raadplegen of delen van kritieke informatie via communicatiekanalen die geen vertrouwelijkheid garanderen, zoals internet e-mail en openbare Wifi netwerken (of zelfs klantnetwerken).
- zorg dat (geprinte) kritieke informatie na gebruik wordt versnipperd.

3.2 Beschermen van informatie van klanten en andere zakenpartners

In het geval Ordina contractuele afspraken heeft gemaakt met de klant/zakenpartner over het beschermen van informatie

Bij het omgaan met informatie van klanten en andere zakenpartners houd je je strikt aan de maatregelen die Ordina met de zakenpartner heeft afgesproken. Als je met gegevens van een klant of zakenpartner werkt, informeer je proactief naar die afspraken.

Toelichting: Vaak maakt Ordina met klanten (en sommige andere zakenpartners) contractuele afspraken over securitymaatregelen. Die afspraken kunnen bijvoorbeeld gaan over het versturen van informatie via de mail, over het afdrukken en het opslaan op mediadragers of over het bewaren c.q. vernietigen van gegevens. Vooral de overheid, de financiële sector en de zorg sector stellen eigen beveiligingseisen bij het uitvoeren van opdrachten.

Voorbeelden van eigen beveiligingseisen:
- Algemene Beveiligingseisen voor Defensieopdrachten (ABDO)
- Baseline Informatiebeveiliging Overheid (BIO)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR)

Je houdt je aan de contractuele afspraken met de klant/zakenpartner als die afspraken verder gaan dan de regels die gelden voor gevoelige informatie van Ordina. Gaan de afspraken met de klant/zakenpartner minder ver dan de regels die gelden voor gevoelige informatie van Ordina, dan neem je toch minimaal de regels in acht die Ordina hanteert voor haar eigen gevoelige informatie zoals vermeld onder 3.1 (tenzij vaststaat dat het om informatie gaat die publiek beschikbaar is).

In het geval Ordina geen contractuele afspraken heeft gemaakt met de klant/zakenpartner over het beschermen van informatie

Als er geen contractuele afspraken zijn met de klant/zakenpartner over het beschermen van informatie neem je minimaal de regels in acht die Ordina hanteert voor haar eigen gevoelige informatie, zoals vermeld onder 3.1 (tenzij vaststaat dat het om informatie gaat die publiek beschikbaar is).

4 Delen van informatie

4.1 Delen van Ordina informatie

Ongevoelige informatie van Ordina mag je met iedereen delen, zowel intern als extern.

Voor **gevoelige informatie** van Ordina geldt dat je deze intern alleen mag delen op basis van het 'need to know' beginsel. Dit betekent dat je de informatie uitsluitend mag delen met collega's die de informatie nodig hebben voor het uitvoeren van hun werkzaamheden. Je deelt gevoelige informatie van Ordina in beginsel niet extern. Je praat dus ook niet met je partner of met familie en vrienden over dergelijke informatie.

Als het in het belang van Ordina is om gevoelige informatie met derden te delen (bijvoorbeeld in het kader van een samenwerking) zorg je dat de ontvanger van de informatie de verplichting heeft om die geheim te houden c.q. te beschermen bijvoorbeeld door het laten tekenen van een geheimhoudingsovereenkomst. Gebruik hiervoor de standaard geheimhoudingsovereenkomst of neem contact op met de afdeling Legal.

Voor **kritieke informatie** van Ordina geldt dat je deze intern alleen mag delen met de personen die specifiek als geautoriseerd worden aangewezen door de persoon die de informatie heeft gecreëerd. Als niet duidelijk is wie specifiek geautoriseerd is, vraag hier dan naar bij degene die de informatie heeft gecreëerd.

Je deelt kritieke informatie van Ordina in beginsel niet extern. Je praat dus ook niet met je partner of met familie en vrienden over dergelijke informatie.

Voor het extern delen van kritieke informatie vraag je vooraf toestemming van de persoon die de informatie heeft gecreëerd. Om zeker te stellen dat de ontvanger van de kritieke informatie deze geheim zal houden dien je de ontvanger een geheimhoudingsovereenkomst te laten tekenen. Gebruik hiervoor de standaard geheimhoudingsovereenkomst of neem contact op met de afdeling Legal.

4.2 Delen van informatie van klanten en andere zakenpartners

Ongevoelige informatie van klanten/zakenpartners

Bedenk dat informatie van klanten/zakenpartners in eerste instantie minimaal als gevoelig moet worden beschouwd. Pas als je hebt vastgesteld dat de informatie al publiek beschikbaar is, kun je deze als ongevoelig beschouwen en mag je deze intern (en extern) delen. Vraag zo nodig de klant/zakenpartner om advies.

Gevoelige informatie van klanten/zakenpartners

Binnen Ordina deel je gevoelige informatie van klanten/zakenpartners alleen op basis van het 'need to know' beginsel. Dit betekent dat je de informatie alleen deelt met collega's die de informatie nodig hebben om de met de klant/zakenpartner contractueel afgesproken werkzaamheden uit te voeren. Je informeert proactief naar die afspraken als je informatie wilt delen.

Als je de informatie met personen buiten deze kring van Ordina collega's wilt delen, heb je toestemming nodig van de klant.
NB: Afgezien van de toestemming van de klant kan het in bepaalde gevallen in strijd zijn met de wet om informatie van de klant te delen; denk aan een aanbestedingsproces waarbij Ordina geen gebruik mag maken van informatie waarover andere concurrenten niet beschikken. Zie hiervoor de richtlijn Eerlijke mededinging.

Mocht het in het belang van de klant/zakenpartner zijn om gevoelige informatie extern met derden te delen (bijvoorbeeld in het kader van een samenwerking) zorg dan dat de ontvanger van de informatie de verplichting heeft om die geheim te houden c.q. te beschermen. Voordat je informatie extern deelt, stem je eerst af met de betreffende klant/zakenpartner.

Kritieke informatie van klanten/ zakenpartners

Extreme voorzichtigheid is geboden bij het delen van kritieke informatie van klanten/zakenpartners. Je deelt dergelijke informatie uitsluitend met collega's als dit absoluut noodzakelijk is voor het verrichten van de contractueel overeengekomen werkzaamheden. Bedenk dat het vele malen beter is om een keer extra bij de klant/zakenpartner te checken of informatie mag worden gedeeld, dan de informatie te delen met een persoon voor wie de informatie niet bedoeld is.

Je deelt kritieke informatie van klanten/ zakenpartners niet extern. Je praat dus ook niet met je partner of met familie en vrienden over dergelijke informatie.

5. Specifieke situaties

Hierna vind je een aantal situaties beschreven waar jij mee te maken kunt krijgen. Per situatie is aangegeven hoe om te gaan met informatie.

5.1 Je wordt gevraagd een persoonlijke geheimhoudingsovereenkomst te tekenen

Het kan voorkomen dat een opdrachtgever je op persoonlijke titel vraagt een geheimhoudings-overeenkomst te tekenen. Dit is dan bovenop een geheimhoudingsplicht die contractueel tussen Ordina en de klant bestaat. (En bovenop de geheimhoudingsplicht in je arbeidsovereenkomst met Ordina). Het risico bestaat dat de overeenkomsten elkaar tegenspreken of dat afspraken worden gemaakt die niet werkbaar zijn. Daarom geldt:

- Vraag advies aan de afdeling Legal voordat je een persoonlijke geheimhoudingsovereenkomst met klanten tekent.

Als je op persoonlijke titel een geheimhoudingsovereenkomst hebt getekend, houd je je natuurlijk aan die afspraken.

5.2 Je bent door Ordina ingezet bij een klant

Als Ordina jou inzet bij een klant, verandert je positie zowel ten aanzien van Ordina als ten aanzien van de klant. Je dient Ordina dan te beschouwen als een derde partij. In deze situatie geldt:

- Je houdt je aan de geheimhoudingsverplichtingen zoals de klant die intern hanteert en aan de verplichtingen die Ordina voor jou heeft afgesproken in de inzetovereenkomst met de klant, of – als je zelf een

geheimhoudingsovereenkomst hebt getekend – aan die individuele afspraken.

Als je die afspraken niet (voldoende) kent, informeer je naar de inhoud van die afspraken bij je inzetverantwoordelijke.

Als je informatie van de klant wilt delen met Ordina collega's, vraag je hiervoor vooraf toestemming aan de klant (tenzij vaststaat dat het om informatie gaat die publiek beschikbaar is). Om discussie achteraf te voorkomen is het nodig dat die toestemming ergens uit blijkt. Je kunt de klant vragen de afspraak te bevestigen, maar je kunt ook zelf bevestigen wat je hierover afspreekt met de klant.

Voorbeeld*:* Je bent aan het werk bij de klant. Tijdens het teamoverleg komt aan de orde dat een aantal ICT diensten binnenkort zal worden uitbesteed. De volgende dag spreek je de inzetverantwoordelijke van Ordina die vraagt of er nog nieuws is.

Vraag: Wat doe je?

Antwoord: Je vertelt je inzetverantwoordelijke pas over de plannen, nadat je met je leidinggevende bij de klant hebt gesproken en die heeft laten weten dat het akkoord is om dit met Ordina te delen. Je stuurt een mailtje ter bevestiging aan de leidinggevende van de klant.

NB: Afgezien van de toestemming van de klant kan het in bepaalde gevallen in strijd zijn met de wet om informatie van de klant te delen; denk bijvoorbeeld aan een aanbestedingsproces waarbij Ordina geen gebruik mag maken van informatie waarover andere concurrenten niet beschikken. Zie hiervoor de richtlijn 'Eerlijke mededinging'.

5.3 Je bent onderdeel van een Ordina projectteam dat voor de klant werkt al dan niet op locatie (je bent niet gedetacheerd)

Wanneer jij aan een opdracht voor een klant werkt, krijg je waarschijnlijk veel informatie van de klant te horen en te zien. Bijvoorbeeld omdat je toegang hebt tot het intranet of bepaalde systemen van de klant of omdat je deelneemt aan vergaderingen.

Natuurlijk gebruik je de informatie die je hoort en ziet voor de uitvoering van de opdracht. Je mag die informatie ook delen met je projectteam op basis van het 'need to know' beginsel (dus met collega's die de informatie nodig hebben voor het uitvoeren van de contractueel overeengekomen werkzaamheden). Maar, als je die informatie binnen Ordina verder deelt dan het projectteam dan moet je toestemming hebben van de klant.

NB: Afgezien van de toestemming van de klant kan het in bepaalde gevallen in strijd zijn met de wet om informatie van de klant te delen; denk aan een aanbestedingsproces waarbij Ordina geen gebruik mag maken van informatie waarover andere concurrenten niet beschikken. Zie hiervoor de richtlijn Eerlijke mededinging.

6. Heb je vragen of twijfels?

Heb je vragen of twijfels over hoe te handelen in een bepaalde situatie? Neem dan altijd contact op met je leidinggevende of de Compliance Officer.

Bij niet naleven van deze richtlijn 'Omgaan met informatie' kan Ordina disciplinaire maatregelen treffen.

Deze richtlijn hangt samen met:

- Algemene Arbeidsvoorwaarden
- Informatiebeveiligingsbeleid en bijbehorende richtlijnen
- Baseline Gedragsregels Informatiebeveiliging
- Archiveringsbeleid (Record Retention Policy)
- Reglement inzake voorwetenschap
- Richtlijn 'Eerlijke mededinging'