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.

Vanuit het perspectief van informatiebeveiliging wordt veelal gesproken over de **B**eschikbaarheid, data -**I**ntegriteit en **V**ertrouwelijkheid van informatie en informatiesystemen (BIV). Zie hiervoor het Informatiebeveiligingsbeleid en bijbehorende richtlijnen.

Het begrip informatie kan op verschillende manieren worden benaderd. De interne richtlijnen Classificatie gaat bijvoorbeeld in op de verschillende soorten informatie.

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.

Deze richtlijn is opgesteld om je te helpen bij het omgaan met informatie. 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 beschreven welke soorten informatie Ordina onderscheidt (classificatie) en of/hoe je die moet labellen. 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. De Quick reference card (Bijlage 1) bevat een korte samenvatting van deze richtlijn.

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 labellen.

Labellen vindt plaats door:
- Vermelding classificatie op het fysieke document: denk aan voorzijde en/of watermerk;
- Vermelding classificatie bij (elektronische) opslag/ registratie: denk aan het in kaart brengen van soorten gegevens binnen (delen van) informatiesystemen.

Classificatietabel*

Mate van gevoeligheid ↓	Vertrouwelijkheid	Classificatie Ordina	Is labellen noodzakelijk?	Delen met
Hoog	(Bedrijfs)belangen[1] worden ernstig geschaad als ongeautoriseerden toegang krijgen.	Kritiek/ Strictly Confidential	Noodzakelijk-	Alleen specifiek benoemde personen
Middel	(Bedrijfs)belangen worden geschaad als ongeautoriseerden toegang krijgen	Gevoelig/ Confidential	Gewenst	Op basis van 'need to know' beginsel[2]
Laag	(Bedrijfs)belangen worden niet geschaad bij openbaarmaking	Ongevoelig/ Unclassified	Niet Noodzakelijk	Iedereen

*Bovenstaande tabel is een gedeeltelijke weergave van de classificatietabel zoals opgenomen in de richtlijnen Classificatie; zie voor de complete tabel de richtlijnen Classificatie.

2.1 Ongevoelige informatie

Kenmerkend voor ongevoelige informatie is dat er geen (bedrijfs)belangen worden geschaad als de informatie publiek bekend wordt. Publieke bronnen zoals kranten en internet bevatten per definitie ongevoelige informatie.

- Als je ongevoelige informatie creëert hoef je die niet te labellen.

Voorbeelden van ongevoelige informatie:
- *jaarverslagen*
- *informatie op de (externe) website van bedrijven*
- *persberichten (**NB**: persberichten gaan vaak over belangrijke onderwerpen; een persbericht is pas ongevoelig **nadat** het naar de pers is gestuurd. Voor die tijd is een persbericht juist vaak kritiek)*

Vraag: Is alle niet-gelabelde Ordina informatie ongevoelig?

Antwoord: Nee. Je mag er niet automatisch van uitgaan, dat het daadwerkelijk ongevoelige informatie is. Check de inhoud van de informatie voordat je die gebruikt of deelt. Vraag zo nodig de maker van de informatie of je leidinggevende om advies.

.

Vraag: Hoe zit het met niet-gelabelde informatie van klanten en andere zakenpartners?

Antwoord: Dergelijke informatie moet je minimaal als gevoelig beschouwen. Alleen als je hebt kunnen vaststellen dat het gaat om informatie die al publiek beschikbaar is, kun je dergelijke informatie als ongevoelig beschouwen. Vraag zo nodig de klant/zakenpartner om advies.

[1] Onder (bedrijfs)belangen verstaan we ook de belangen van onze zakenpartners en medewerkers o.a. waar het persoonsgegevens betreft.
[2] 'Need to know' beginsel: informatie van Ordina mag uitsluitend met collega's worden gedeeld die de informatie nodig hebben voor het uitvoeren van hun werkzaamheden; informatie van klanten/ zakenpartners mag uitsluitend met collega's worden gedeeld die de informatie nodig hebben voor het uitvoeren van de contractueel met die klanten/ zakenpartner overeengekomen werkzaamheden.

2.2 Gevoelige informatie

Kenmerkend voor gevoelige informatie is dat (bedrijfs)belangen worden geschaad wanneer ongeautoriseerden toegang krijgen tot die informatie.

Informatie kan bovendien gevoelig zijn enkel op grond van de wet; dit geldt bijvoorbeeld voor persoonsgegevens (m.u.v. bijzondere persoonsgegevens zoals medische informatie; die is namelijk kritiek).

- Als je gevoelige informatie creëert is het **gewenst** om die te labellen (bijvoorbeeld als '*vertrouwelijk'* of '*uitsluitend voor intern gebruik*')

.

Voorbeelden gevoelige Ordina gegevens:
- *commerciële documenten zoals marktverkenningen, offertes, OCS*
- *contracten, en de op contracten betrekking hebbende financiële gegevens*
- *projectgegevens zoals PID, stuurgroep verslagen, testresultaten, risico-, issue- en kwaliteitsregisters*
- *bestanden met persoonsgegevens (zonder bijzondere gegevens)*
- *beheergegevens zoals SLA, DAP, SLR, release aanpak, impactanalyses*

Informatie is steeds gevoelig als deze als zodanig is gelabeld.

Vraag: Kan niet-gelabelde Ordina informatie gevoelig zijn?

Antwoord: Ja. Check de inhoud van de informatie voordat je die gebruikt of deelt. Vraag zo nodig de maker van de informatie of je leidinggevende om advies.

Vraag: Hoe zit het met niet-gelabelde informatie van klanten en andere zakenpartners?

*Antwoord: Dergelijke informatie moet je in eerste instantie **minimaal** als gevoelig beschouwen, tenzij je hebt vastgesteld dat de informatie publiek beschikbaar is. Vraag zo nodig de klant/zakenpartner om advies.*

2.3 Kritieke informatie

Kenmerkend voor kritieke informatie is dat (bedrijfs)belangen ernstig worden geschaad wanneer ongeautoriseerden toegang krijgen tot die informatie. Informatie kan bovendien kritiek zijn enkel op grond van de wet; dit geldt bijvoorbeeld voor bijzondere persoonsgegevens, zoals medische informatie.

Soms is de classificatie' kritiek' afhankelijk van het tijdstip waarop je over die informatie beschikt. De jaarcijfers (en kwartaal-, en halfjaarcijfers) van Ordina zijn bijvoorbeeld kritiek tot het moment dat deze gepubliceerd worden. Na publicatie zijn die gegevens juist ongevoelig (want publiek bekend).

- Als je kritieke informatie creëert moet je die labellen als '*kritiek'* of '*strikt vertrouwelijk'*. Je moet ook bepalen voor welke specifiek benoemde personen de informatie bedoeld is.

Voorbeelden van kritieke gegevens:
- *personeelsdossiers*
- *medische gegevens*
- *plannen voor overnames of reorganisaties*
- *managementrapportages*

Informatie die als' *kritiek'* of '*strikt vertrouwelijk'* is gelabeld, moet je altijd als kritiek beschouwen.

Vraag: Kan niet-gelabelde Ordina informatie kritiek zijn?

Antwoord: Ja. Men kan vergeten zijn de informatie als kritiek te labellen. Check de inhoud van de informatie voordat je die gebruikt of deelt. Vraag zo nodig de maker van de informatie of je leidinggevende om advies.

Vraag: Kan niet-gelabelde informatie van klanten en andere zakenpartners kritiek zijn?

Antwoord: Ja. Dergelijke informatie moet je in eerste instantie minimaal als gevoelig beschouwen, maar kan kritiek zijn. Blijkt de informatie kritiek te zijn, label deze dan alsnog en vraag de klant/zakenpartner om advies hoe te handelen.

2.4 Twijfel je over de juiste classificatie?

Als je twijfelt over het classificatieniveau van bepaalde informatie behandel je die gegevens **minimaal** als gevoelig, totdat je de kans hebt gehad een en ander te verifiëren bij je leidinggevende of bij de klant/zakenpartner.

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 tot en met 3.3.

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 Rijksdienst (BIR)*
- *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
- Privacy reglement verwerking persoonsgegevens
- Richtlijn classificatie
- Archiveringsbeleid (Record Retention Policy)
- Richtlijn mobiele apparatuur en gegevensdragers
- Reglement inzake voorwetenschap
- Richtlijn ‘Eerlijke mededinging’

Bijlage 1. – Quick reference card

Soorten informatie - hoofdstuk 2

Classificatietabel*

Mate van gevoeligheid ↓	Vertrouwelijkheid	Classificatie Ordina	Is labellen noodzakelijk?	Delen met
Hoog	(Bedrijfs)belangen[3] worden ernstig geschaad als ongeautoriseerden toegang krijgen.	Kritiek/ Strictly Confidential	Noodzakelijk-	Alleen specifiek benoemde personen
Middel	(Bedrijfs)belangen worden geschaad als ongeautoriseerden toegang krijgen	Gevoelig/ Confidential	Gewenst	Op basis van 'need to know' beginsel[4]
Laag	(Bedrijfs)belangen worden niet geschaad bij openbaarmaking	Ongevoelig/ Unclassified	Niet Noodzakelijk	Iedereen

*Deze tabel is een gedeeltelijke weergave van de classificatietabel zoals opgenomen in de richtlijnen Classificatie; zie voor de complete tabel de richtlijnen Classificatie.

Gedragsregels voor het beschermen van informatie – hoofdstuk 3

	informatie van Ordina		informatie van zakenpartners
altijd	• clear-desk • clean-screen • vergrendel mobiele apparaten • beperk hoeveelheid data op je laptop • gebruik USB harddisk alleen voor eigen data op je laptop • zorg dat eigen devices (BYOD) aan dezelfde eisen voldoen als Ordina devices; • meld verlies of diefstal dadelijk		• Je houdt je aan de contractuele afspraken met de zakenpartner; • als de afspraken met de zakenpartner minder ver gaan dan de regels die gelden voor **gevoelige** informatie van Ordina – of als er geen contractuele afspraken zijn - neem je tenminste de regels in acht die gelden voor **gevoelige** informatie van Ordina (tenzij
gevoelige informatie	**additioneel** • ga zorgvuldig om met autorisaties; • berg gevoelige (geprinte) informatie veilig op of gooi weg in afgesloten papierbak weggooien		
kritieke	**additioneel**		

[3] Onder (bedrijfs)belangen verstaan we ook de belangen van onze zakenpartners en medewerkers o.a. waar het persoonsgegevens betreft.
[4] 'Need to know' beginsel: informatie van Ordina mag uitsluitend met collega's worden gedeeld die de informatie nodig hebben voor het uitvoeren van hun werkzaamheden; informatie van klanten/ zakenpartners mag uitsluitend met collega's worden gedeeld die de informatie nodig hebben voor het uitvoeren van de contractueel met die klanten/ zakenpartner overeengekomen werkzaamheden.

informatie	• mag alleen op een mobile device als de encryptie (gegevenscodering) aan de meest recente Ordina data encryption standards voldoet; • vermijd onveilige communicatiekanalen (zoals openbare Wifi); • versnipper geprinte kritieke info na gebruik		vaststaat dat het om informatie gaat die publiek beschikbaar is).

Delen van Ordina informatie – hoofdstuk 4.1

type informatie	intern delen	extern delen
ongevoelige	toegestaan	toegestaan
gevoelige	alleen op basis van 'need to know' beginsel	niet, tenzij in het belang van Ordina en beschermd door geheimhoudingsovereenkomst
kritiek/strikt vertrouwelijk	intern alleen met specifiek geautoriseerde medewerkers	niet, tenzij met voorafgaande toestemming van degene die informatie gecreëerd heeft en beschermd door geheimhoudingsovereenkomst

Delen van informatie van klanten en andere zakenpartners – hoofdstuk 4.2

type informatie	intern delen	extern delen
ongevoelig NB: ongevoelig is alleen informatie waarvan je hebt vastgesteld dat deze publiek beschikbaar is	toegestaan	toegestaan
gevoelig in beginsel valt alle informatie van klanten minimaal in deze categorie	alleen met medewerkers die informatie nodig hebben om de contractueel met de klant afgesproken werkzaamheden uit te voeren **OF** met toestemming van de klant[5]	niet, tenzij met toestemming van de klant en beschermd door geheimhoudingsovereenkomst
kritiek/strikt vertrouwelijk	alleen met medewerkers die informatie absoluut nodig hebben om de contractueel met de klant afgesproken werkzaamheden uit te voeren **OF** met toestemming van de klant[6]	niet

[5] 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] idem