INFORMATIE & BEVEILIGINGSBELEID

THERE'S MORE
THAN MEETS THE EYE

wink

EEN BEVEILIGINGSBELEID...?

Als wij werkzaamheden voor je uitvoeren, vertrouw je ons met jouw gegevens en die van je klanten. Het is onze verantwoordelijkheid om daar op een juiste manier mee om te gaan, en om je inzicht te geven in hoe we dat doen.

In dit document zetten we onze richtlijnen t.a.v. de beveiliging die we hanteren op een rijtje. Wel zo duidelijk! Mocht je nog vragen hebben naar aanleiding van dit document, neem dan zeker even contact met ons op!

INHOUDSOPGAVE

JOUW GEGEVENS.

In het kader van de werkzaamheden die Wink uitvoert voor haar klanten, worden vaak gegevens aangeleverd en verwerkt. We maken onderscheid tussen drie soorten gegevens:

1. Klantgegevens
2. (Privacy)gevoelige informatie (vertrouwelijk)
3. Overige gegevens

1. Klantgegevens

Onder klantgegevens verstaan we jouw NAW- en bedrijfsgegevens die wij opslaan t.b.v. de (administratieve) afhandeling en nazorg rondom het uitvoeren van een overeenkomst. Bijvoorbeeld: Je (bedrijfs)naam, KvK- en BTW-nummer, factuuradres.

Verwerking

Je gegevens worden verwerkt in onze interne systemen en komen tot uiting op bijvoorbeeld offertes en facturen. Deze gegevens slaan we op voor onbepaalde termijn.

Na het beëindigen van onze samenwerking

Op verzoek verwijderen we jouw klantgegevens na het beëindigen van onze samenwerking en zodra de wettelijk verplichte bewaartermijnen verstreken zijn.

We gaan zorgvuldig met je gegevens om
en bewaren (privacy)gevoelige informatie
niet langer dan strikt noodzakelijk.

2. (Privacy)gevoelige informatie (vertrouwelijk)

Deze aanduiding geven wij en/of jij aan informatie die persoonsgegevens bevat of een sterk vertrouwelijk karakter heeft.
Bijvoorbeeld: Een lijst van e-mailadressen of een Excel bestand met financiële informatie. Of een willekeurig ander document door u aangemerkt als 'vertrouwelijk'.

Aanduiding vertrouwelijk

Wanneer je gegevens aanlevert die jij als vertrouwelijk beschouwt, dan verwachten we dat jij dat duidelijk aangeeft. Wanneer wij informatie ontvangen met persoonsgegevens (bijv: NAW-gegevens, e-mailadressen of IP adressen), dan zullen wij deze informatie aanmerken als (privacy)gevoelig.

We verwachten in beide gevallen dat de aanlevering geschiedt via de daarvoor bestemde oplossing (zie 'Aanlevering' hieronder). Wanneer je ons (privacy)gevoelige informatie stuurt via een andere weg, bijvoorbeeld een e-mail, dan zullen we de ontvangen informatie per direct verwijderen en je vragen om de informatie alsnog via onderstaande oplossing aan te leveren.

Aanlevering

Wanneer je persoonsgegevens of anderszins gevoelige informatie wil aanleveren ter verwerking, vereisen we dat deze informatie op een veilige manier aangeleverd wordt. Wink biedt hiertoe een voorziening: Als klant kun je inloggen op het Wink klantportaal op https://klanten.winkdigital.nl. Daar kun je vervolgens dit soort gegevens uploaden. De aanlevering geschiedt daarmee digitaal over een beveiligde en versleutelde verbinding. Informatie over de aanlevering en verdere verwerking door ons wordt bijgehouden en inzichtelijk gemaakt voor jou.

Verwerking

Wanneer je ons gegevens hebt aangeleverd via de beveiligde online omgeving, worden ze tijdelijk bewaard op één van onze servers. Zodra wij de gegevens gaan verwerken, worden ze ingeladen op een werkplek en na verwerking

verwijderd van beide locaties. De status van verwerking en – uiteindelijk – het verwijderen van de aangeleverde gegevens, wordt bijgehouden in het Wink klantportaal en is daarmee voor jou inzichtelijk.

Aflevering

Indien door jou aangevraagd, kan Wink vertrouwelijke informatie in de vorm van exports aan je sturen. Aflevering van bestanden met vertrouwelijke informatie of persoonsgegevens zal altijd plaatsvinden via het klantportaal. Je ontvangt via e-mail een bericht dat er bestanden klaar staan. Na inloggen op het klantportaal download je de bestanden via een versleutelde en beveiligde verbinding. Bestanden die Wink voor je klaar zet ter aflevering, kennen een beperkte houdbaarheid: bestanden worden automatisch verwijderd 7 dagen na uploaden.

3. Overige gegevens

Alle overige gegevens die we verwerken voor je.
Bijvoorbeeld: Teksten of foto(grafisch) materiaal ter publicatie, productinformatie t.b.v. het vullen van een webshop. Of andere inhoudelijke informatie niet aangemerkt als vertrouwelijk.

Aanlevering

Voor alle overige gegevens accepteren we uitsluitend een digitale aanlevering.
Voor gegevens die geen strikte geheimhouding vereisten, volstaat aanleveren via:
- een e-mail met bijlage
- een transfer via een dienst als OneDrive of WeTransfer

We accepteren geen fysieke dragers zoals USB sticks, CD/DVD's of externe harde schijven.

Na het beëindigen van onze samenwerking

Wink bewaart deze gegevens zolang we samen werken. Na het beëindigen van onze samenwerking zullen je overige gegevens, na een onbepaalde termijn, verwijderd worden. Op verzoek dragen we er zorg voor dat deze gegevens binnen 14 dagen verwijderd worden.

JOUW GEGEVENS: IN EEN NOTENDOP.

We gaan zorgvuldig met je gegevens om en bewaren (privacy)gevoelige informatie niet langer dan strikt noodzakelijk.

Vertrouwelijk en/of (privacy)gevoelig

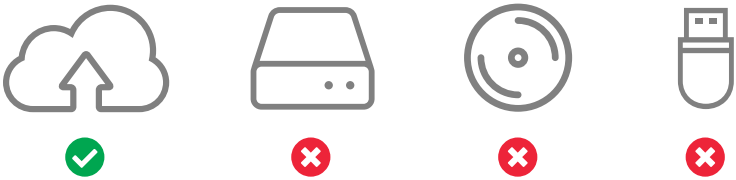
Wanneer je ons informatie aanlevert die vertrouwelijk is, gaan we er vanuit dat jij deze gegevens duidelijk aanmerkt als vertrouwelijk. Wanneer de door jou aangeleverde informatie persoonsgegevens bevat, dan beschouwen wij dit automatisch als privacy-gevoelig.

Beveiligd aanleveren

Lever vertrouwelijke of (privacy)gevoelige informatie aan via het klantportaal op https://klanten.winkdigital.nl.

Digitaal aanleveren

Lever ons bij voorkeur alles digitaal aan. We accepteren geen fysieke dragers zoals USB sticks, CD/DVD's of externe hdd's.



ONZE WERKPLEKKEN.

Fysieke werkplekken

De werkzaamheden die we voor je uitvoeren, voeren we te allen tijde uit op een daarvoor aangemerkte 'werkplek'. Dat is veelal een vaste fysieke werkplek bij ons op locatie, maar dat kan ook een plek op jouw locatie zijn, wanneer we je daar ondersteunen.

Toegang

In het geval van een vaste werkplek, bijvoorbeeld bij ons op locatie of een thuiswerkplek, dan wordt toegang tot deze werkplek verschaft op persoonsniveau. In het geval dat we je ondersteunen op locatie (en dus werken vanaf een flexibele werkplek), ben jij verantwoordelijk voor het verschaffen van fysieke toegang.

Clean Desk Policy

Op het einde van de werkdag wordt de werkplek geordend en opgeruimd achtergelaten. We zorgen ervoor dat alle gevoelige en/of vertrouwelijke informatie in hardcopy of elektronische vorm bij het verlaten van de werkplek veilig opgeborgen is en niet toegankelijk voor onbevoegden.

In het geval dat we je ondersteunen op locatie, dan verwachten we dat er een opgeruimde werkplek ter beschikking gesteld wordt, waar zich geen (privacy) gevoelige gegevens bevinden.

Door bewust om te gaan met onze werkplekken
en apparatuur houden we grip op jouw en onze informatie.

Paperless culture
We vermijden het gebruik van papier en hardcopy gegevens; we werken zo veel als mogelijk digitaal.

Printergebruik
Afdrukken met (privacy)gevoelige informatie worden niet onbeheerd in een printer achtergelaten. We vermijden het gebruik van papier en hard-copy gegevens en we werken zo veel als mogelijk digitaal.

Netwerk
Toegang tot het draadloos of bekabelde netwerk op een Wink locatie wordt beperkt tot de medewerkers van Wink. Aan derden wordt uitsluitend toegang tot internet verschaft via het gastnetwerk.

Afvoeren van (privacy)gevoelige gegevens
Bij het afvoeren van hardcopy (privacy)gevoelige gegevens wordt gebruik gemaakt van een papiershredder indien aanwezig. Op onze vaste werkplekken is deze voorziening aanwezig. In het geval dat we je ondersteunen op locatie, ben jij verantwoordelijk voor het veilig afvoeren van deze gegevens.

Computergebruik
Onze werkzaamheden voeren we uitsluitend uit op computers die zijn aangemerkt als bedrijfsapparatuur. Dit betreft in alle gevallen een door ons verstrekt apparaat. Voor het gebruik van deze apparatuur hanteren wij de volgende regels.

Clear Screen Policy
Bij afwezigheid worden computerwerkplekken vergrendeld. Op het einde van de werkdag worden computerwerkplekken afgesloten indien mogelijk.

Full-disk encryptie
We verwerken en bewaren jouw gegevens alleen op schijven die versleuteld zijn d.m.v. full-disk encryptie technologieën zoals Bitlocker.

Geen (onbeveiligde) externe dragers

We vermijden het gebruik van externe dragers zoals USB sticks, optische media, of externe harde schijven. We maken in het geheel geen gebruik van onbeveiligde dragers voor (privacy)gevoelige of vertrouwelijke informatie.

Updates en antivirus

Onze computers worden voorzien van een operating system (OS) dat officiële ondersteuning geniet. Dit OS wordt up-to-date gehouden en voorzien van een up-to-date antivirus oplossing.

Openbare netwerken

Er wordt in de regel geen gebruik gemaakt van onbeveiligde netwerken. Wanneer dat wel het geval is, werken we uitsluitend via beveiligde verbindingen.

Overige apparatuur

Er zijn mogelijk andere apparaten die gebruikt worden door Wink medewerkers voor taken als het uitlezen van e-mail (bijvoorbeeld: smartphones of tablets). Indien een Wink account ingeladen wordt op een dergelijk apparaat, is het een vereiste dat de toegang tot het apparaat of het account afgeschermd wordt met een wachtwoord, pincode of biometrische identificatie.

Privacy(gevoelige) of vertrouwelijke informatie wordt niet verwerkt op deze apparaten (uitsluitend op bedrijfsapparatuur).

ONZE WERKPLEKKEN: IN EEN NOTENDOP.

We verwerken (privacy)gevoelige informatie uitsluitend op aangewezen werkplekken en aangewezen bedrijfsapparatuur.

Fysieke werkplekken

We werken veelal vanuit onze vaste werkplekken bij ons op locatie, maar we kunnen je ook ondersteunen op jouw locatie. In beide gevallen werken we in een opgeruimde en geordende omgeving en vermijden we het werken met hard-copy gegevens.

Beveiligde apparatuur

Onze apparatuur is te allen tijde beveiligd en wordt niet onvergrendeld verlaten. We zijn selectief in het verlenen van toegang.

ONZE SERVERS.

Wij maken gebruik van servers voor diverse doeleinden, bijvoorbeeld voor het hosten van websites en webapplicaties, het afhandelen van e-mailverkeer en het uitvoeren van geautomatiseerde back-up taken.

Toegang - beheer

Wanneer er beheer-taken uitgevoerd worden op onze servers, gebeurt dit uitsluitend via een beveiligde en versleutelde verbinding vanaf onze werkplekken. De accounts waarmee we werken zijn te allen tijde beveiligd met sterke en unieke wachtwoorden.

Fysiek beheer

Voor het fysieke beheer van onze servers werken we samen met vertrouwde leveranciers en datacentra binnen Nederland. De datacentra waarin de servers geplaatst zijn, gaan zorgvuldig om met hun beveiliging. De datacentra bezitten de volgende certificeringen:

ISO 9001	ISO 27001	ISO 14001	NEN 7510	PCI DSS

Toegang voor derden

Er wordt in de regel geen toegang verschaft aan derden in het kader van beheertaken. Wanneer dit wel noodzakelijk is, zal er toegang verschaft worden op persoonsniveau en wordt de toegang beperkt tot hetgeen nodig is voor het uitvoeren van de werkzaamheden.

Onze web-, mail- en back-up servers zijn geplaatst in een beveiligde omgeving, zowel digitaal als fysiek.

Toegang - Operationeel

Er kan toegang verschaft worden aan derden tot bepaalde onderdelen en protocollen op onze servers in een operationeel kader. Toegang wordt in dat geval verschaft op persoonsniveau en voor beperkte onderdelen.

Toegang tot een klantomgeving

Wanneer er toegang verschaft wordt tot een omgeving met gegevens van een specifieke klant, wordt die toegang uitsluitend verstrekt aan de klant, via een beveiligd protocol en sterke, unieke, wachtwoorden. Indien de klant zelf de mogelijkheid heeft om het wachtwoord te wijzigen, dan raden we aan z.s.m. een eigen wachtwoord te kiezen. De klant is in dit geval verantwoordelijk voor het hanteren van een sterk wachtwoord.

Als richtlijn voor een sterk wachtwoord kan het volgende aangehouden worden:

- minimaal 12 tekens lang
- een mix van hoofdletters, kleine letters, cijfers en leestekens
- bevat geen voor de hand liggende informatie als geboortedata of adressen
- een uniek wachtwoord dat op geen enkele andere plek gebruikt wordt

Update-beleid

Onze servers zijn voorzien van een operating system (OS) dat officiële ondersteuning geniet. Reguliere updates worden periodiek doorgevoerd. Wanneer kritieke beveiligingslekken ontdekt worden in de gebruikte software, worden de patches daarvoor na uitgifte z.s.m. aangebracht.

ONZE SERVERS: IN EEN NOTENDOP.

Onze web-, mail- en back-up servers zijn geplaatst in een beveiligde omgeving, zowel digitaal als fysiek.

Fysieke locatie

We werken samen met vertrouwde leveranciers en gecertificeerde datacentra binnen Nederland voor het fysieke beheer van onze servers.

Toegang

We verlenen in de regel geen toegang aan derden en werken uitsluitend via beveiligde verbindingen en accounts met unieke, sterke wachtwoorden.

Updates

Servers worden bijgewerkt via een update-beleid om optimale performance en beveiliging te kunnen garanderen.

DE BACKUPS.

We maken geautomatiseerd back-ups van jouw en onze gegevens on-site en naar diverse off-site locaties. De inhoud van onze werkplekken en servers wordt op die manier veilig gesteld. Off-site back-ups zijn te allen tijde aanwezig op minimaal 3 fysieke locaties. Deze back-up doelen zijn, net als onze werkplekken, voorzien van full-disk encryptie. Toegang tot deze servers wordt beperkt tot onze medewerkers.

Historie
Geautomatiseerde back-up taken zorgen ervoor dat gegevens op een regelmatig interval bewaard worden. Van sommige gegevens bewaren we tevens de historie. In dat geval bewaren we de gegevens en veranderingen daarvan over een periode van 240 dagen.

(Privacy)gevoelige informatie
Wanneer (privacy)gevoelige gegevens verwijderd worden, zullen ze kort daarna automatisch verwijderd worden op de reguliere back-up doelen. Wanneer deze gegevens onderdeel uitmaken van een back-up taak met behoud van historie, worden ze voor een periode van 240 dagen bewaard na het lokaal verwijderen.

Zorgvuldig omgaan met gegevens beperkt zich niet alleen tot de beveiliging daarvan. Ook het veilig bewaren is van belang.

DE BACKUPS: IN EEN NOTENDOP.

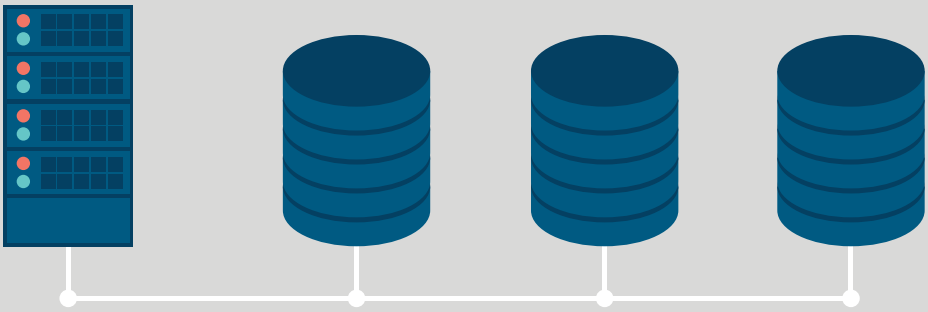
Onze web-, mail- en back-up servers zijn geplaatst in een beveiligde omgeving, zowel digitaal als fysiek.

Off-site back-ups

Onze back-ups zijn te allen tijde beschikbaar op minimaal 3 fysieke locaties.

Historie

Sommige back-up taken worden uitgevoerd met behoud van historie. In dat geval worden gegevens voor 240 dagen bewaard.



ONZE MEDEWERKERS.

Bij in dienst treden

Verklaring omtrent gedrag
Wij verlangen van medewerkers dat zij een verklaring omtrent gedrag aanleveren bij het in dienst treden.

Instructie en geheimhouding
Onze medewerkers worden op de hoogte gebracht van het geldende beveiligingsbeleid en bijbehorende procedures. Verder worden medewerkers gehouden aan een geheimhoudingsplicht m.b.t. (privacy-)gevoelige informatie.

Verschaffen van toegang
Aan medewerkers wordt toegang verschaft tot een werkplek en tot diverse informatiesystemen. Deze toegang wordt via een password manager verleend en beperkt tot hetgeen nodig is voor het uitvoeren van de werkzaamheden.

Bij uit dienst treden

Ontnemen van toegang
Bij de beëindiging van een dienstverband zal toegang tot de werkplek en informatiesystemen ontnomen worden. Alle bedrijfsapparatuur wordt verzameld op locatie en terug in beheer genomen door Wink.

We nemen samen een actieve houding in in het waarborgen van een goede informatiebeveiliging.

MEER WETEN?

Heb je verder nog vragen over dit beleid of de manier waarop we jouw gegevens verwerken? Neem dan contact op met ons:

info@winkdigital.nl

046 - 870 00 26

Heerstraat Centrum 131

6171 HV Stein