IN CONTROL
OF LOGISTICS

Verwerkersovereenkomst Vanboxtel B.V.

Bestaande uit:

Deel 1:	Data Pro Statement
Deel 2:	Standaardclausules voor verwerkingen (NLdigital versie maart 2025)

DEEL 1: DATA PRO STATEMENT

Dit data Pro Statement vormt samen met de Standaardclausules voor verwerkingen de verwerkersovereenkomst voor de producten of diensten van het bedrijf dat dit Data Pro Statement heeft opgesteld.

ALGEMENE INFORMATIE

1. **Dit Data Pro Statement is opgesteld door de volgende data processor (verwerker):**
   Vanboxtel B.V., Kerkstraat 4 5427 BC Boekel
   Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met:
   Marc van Lierop, m: mvlierop#vanboxtel.nl, t: +31 (0)492-327333

2. **Dit Data Pro Statement geldt vanaf 11-08-2026**
   Dit Data Pro Statement en de daarin omschreven beveiligingsmaatregelen passen wij regelmatig aan om ten aanzien van data protectie steeds voorbereid en actueel te blijven. Wij houden u op de hoogte van nieuwe versies via onze website.

3. **Dit Data Pro Statement is van toepassing op de volgende producten en diensten van data processor**
   A: Vanboxtel-WMS
   B: Internetverbinding
   C: Netwerk componenten
   D: Warehouse assets

   In de hoofdovereenkomst(en) tussen Data Processor en opdrachtgever is bepaald welke producten/diensten bij Data Processor zijn afgenomen.

4. **Omschrijving producten/diensten**
   A: Het Warehouse Management System (WMS) wordt toegepast voor het beheersen en optimaliseren van de goederenstromen in een magazijn.
   B: De internetverbinding draagt zorg voor de gegevensdoorvoer vanaf de locatie(s) van de opdrachtgever naar de locatie(s) van de opdrachtgever.
   C: De netwerkcomponenten dragen zorg voor de gegevensdoorvoer binnen de locatie(s) van de opdrachtgever zelf.
   D: Middels de warehouse assets kunnen medewerkers van de opdrachtgever gegevens op een eenvoudige wijze vastleggen binnen het WMS.

5. **Beoogd gebruik**
   De producten/diensten zijn ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:
   Voor het beheersen en optimaliseren van de goederenstromen worden de logistieke acties binnen het magazijn aangestuurd en vastgelegd middels het WMS. Dit omvat onder andere de registratie van binnenkomende goederen waaronder leverancier gegevens, en de registratie van uitgaande goederen waaronder afleveradresgegevens. Deze afleveradressen kunnen zowel bestaan uit bedrijven (in dat geval gaat het om B2B-leveringen) als consumenten (in dat geval gaat het om B2C-leveringen). Tevens worden basisgegevens van medewerkers die gebruik maken van het WMS zelf geregistreerd.

   Bij deze producten/diensten is geen rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of door de overheid uitgegeven persoonsnummers.

6. **Privacy by design/privacy by default**
   Standaard is het binnen de systemen van Vanboxtel alleen mogelijk om persoonsgegevens vast te leggen, te tonen en te printen welke strikt noodzakelijk zijn voor de uitvoering van de beoogde diensten. Het kunnen vastleggen van naam en adresgegevens en deze vervolgens te printen op pakbonnen en verzendlabels om het verzenden van goederen naar een afnemer mogelijk te maken is hier een sprekend voorbeeld hiervan.

7. **Data processor gebruikt de Standaardclausules voor verwerkingen, welke als bijlage bij de Overeenkomst te vinden zijn.**

8. **Data processor verwerkt de persoonsgegevens van zijn opdrachtgevers binnen de EU/EER**.

9. **Data processor maakt geen gebruik van sub-processors.**

10. **Opdrachtgever kan Data processor vragen om (delen) van de aanwezige persoonsgegevens te laten corrigeren, te verwijderen dan wel te anonimiseren. Data processor zal een dergelijk verzoek binnen een redelijke termijn realiseren, maar uiterlijk binnen 1 maand.**

11. **Data processor zal binnen 1 maand medewerking verlenen aan een redelijk verzoek van Opdrachtgever tot deelname aan een Data Protection Impact Assessment (DPIA). Data Processor kan de redelijke kosten die hij in dit kader maakt in rekening brengen bij Opdrachtgever tegen zijn dan geldende tarieven.**

12. **Na beëindiging van de Overeenkomst met een opdrachtgever verwijdert data processor de persoonsgegevens die hij voor opdrachtgever verwerkt in principe binnen 3 maanden op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessible).**

13. **Er zijn geen afspraken gemaakt voor het retourneren van persoonsgegevens na beëindiging van de overeenkomst. De persoonsgegevens worden verwijderd conform het gestelde in het vorige punt 11.**

BEVEILIGINGSBELEID

14. **Data processor heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van zijn producten of diensten:**

Security Team
Binnen de organisatie van Vanboxtel is het security Team verantwoordelijk voor het informatiebeveiligingsbeleid ten behoeve van haar producten en diensten. Dit team bestaat uit meerdere medewerkers uit verschillende disciplines binnen Vanboxtel.

Informatiebeveiligingsbeleid
Het security team is verantwoordelijk voor het bepalen van het informatiebeveiligingsbeleid.
Dit team komt periodiek bijeen voor:

- analyse van risico's voor beveiliging en privacy binnen bedrijfsprocessen en uitvoering;
- evaluatie van eerder geïmplementeerde verbetermaatregelen en eventueel daaruit voortvloeiende verbetervoorstellen;
- opstellen concrete verbetervoorstellen en actiepunten voor nieuwe en bestaande risico's;
- verslaglegging.
  Dit team of deel van dit team komt incidenteel bijeen voor:
- Bepalen aanpak voor risico's met hoge prioriteit.

Dit team houdt elkaar continue op de hoogte middels een gezamenlijke mail van alle zaken binnen Vanboxtel welke het informatiebeveiligingsbeleid raakt.

Personeel
Alle medewerkers van Vanboxtel worden gescreend alvorens ze in dienst treden bij Vanboxtel op basis van een Verklaring Omtrent het Gedrag (VOG) en een identificatieplicht. Voor alle medewerkers geldt een geheimhoudingsverklaring als onderdeel van de arbeidsovereenkomst. Medewerkers betrachten strikte geheimhouding van gevoelige gegevens tegenover derden.

Logische toegang
Het Security team is verantwoordelijk voor het beheer van de logische toegang tot belangrijke gegevens met betrekking tot de systemen. Hierbij valt te denken aan toegangscodes, sleutels, toegang via vingerafdruk en wachtwoorden voor servers, software en databases. Wachtwoorden liggen versleuteld vast in een database en zijn enkel opvraagbaar voor medewerkers die voldaan aan een bepaald niveau. Het niveau wordt per medewerker door het security team bepaald en centraal vastgelegd in een rechtensheet. Periodiek of indien noodzakelijk wordt het niveau van een medewerker geëvalueerd en indien nodig aangepast. Van de medewerkers die Vanboxtel verlaten, vervallen alle toegangsrechten.

Datalek
In et geval van een datalek treedt direct het datalekprotocol in werking. Het datalekprotocol is verderop in dit document opgenomen.

Subverwerkers
Vanboxtel maakt ten tijde van het afsluiten van de overeenkomst geen gebruik van subverwerkers. Vanboxtel heeft echter de mogelijkheid om subverwerkers in te schakelen zonder voorafgaande toestemming van de Opdrachtgever. Vanboxtel verzekert Opdrachtgever dat de subverwerker zich richt naar haar instructies, tot geheimhouding verplicht is en de nodige beveiligingsmaatregelen ten opzichte van de gegevensverwerking neemt. Alle relevante verplichtingen uit deze overeenkomst voor de bescherming en beveiliging van de persoonsgegevens worden overgenomen in de overeenkomst met de subverwerker.

Datacenter
Vanboxtel maakt gebruik van eigen servers binnen twee geografisch gescheiden datacenters van Interconnect (Eindhoven en ’s Hertogenbosch). De datacenters van Interconnect zijn ISO 9001, 27001 en 14001 gecertificeerd en daarnaast heeft Interconnect een ISAE 3000 / SOC 2 TYPE 2 verklaring. Tevens committeert Interconnect zich aan de doelstelling om deze zaken doorlopend te monitoren en te verbeteren. De data wordt opgeslagen.

Backup
Vanboxtel maakt gebruik van een gevalideerde backup en recovery methode.

De backup is netwerktechnisch volledig geïsoleerd en gescheiden van de live data van de opdrachtgever. Daarnaast wordt de backup gemaakt op een locatie welke geografisch is gescheiden van de live data van de opdrachtgever.

Beveiligingsmaatregelen
Vanboxtel neemt de verwerking van Persoonsgegevens zeer serieus en neemt passende maatregelen om misbruik, verlies, onbevoegde toegang, ongewenste openbaarmaking en ongeoorloofde wijziging tegen te gaan. Vanboxtel heeft daartoe maatregelen geïmplementeerd met betrekking tot software en infrastructuur:

- Firewall cluster met IPS/IDS per opdrachtgever
- Aparte OTAP omgeving per opdrachtgever
- Automatische Security updates
- Periodieke pentests
- DDoS protectie
- Endpoint protectie
- Vulnerability Management
- Beveiligde verbinding met opdrachtgever

15. **Data processor heeft zich geconformeerd aan het volgende Information Security Management System (ISMS):**
    NEN-ISO 27001

16. **Data processor heeft de volgende certificeringen:**
    Data Pro Verified

DATALEKPROTOCOL

17. In geval er toch iets mis gaat, hanteert data processor het volgende datalekprotocol om ervoor te zorgen dat opdrachtgever op de hoogte is van incidenten:

Deze paragraaf beschrijft de verschillende stappen die binnen Vanboxtel BV genomen worden bij een datalek, welke valt onder de Meldplicht Datalekken. De data processor (Vanboxtel BV) is verplicht om een datalek te melden bij de opdrachtgever.

Mogelijke oorzaken van een datalek zijn bijvoorbeeld:

- Moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, malware);
- Technisch falen (fouten of bugs in software, verlate updates, storingen);
- Menselijk falen (onzorgvuldige omgang gebruikersnaam en/of wachtwoord, nalatigheid;
- Verloren of gestolen hardware (externe harde schijf, USB stick, server-apparatuur of laptop);
- Verzenden e-mail naar onbedoelde mailadressen met openbaring van persoonsgegevens;

Melding

Alle datalekken van persoonsgegevens dienen intern te worden gemeld bij en worden gedocumenteerd door een lid van het Team Security. De melding kan door iedere gebruiker, iedere medewerker of derde partij worden gedaan bij een medewerker van Vanboxtel. De melding wordt vervolgens door de melder zelf of door de betrokken medewerker direct telefonisch doorgegeven aan een lid van Team Security en schriftelijk vastgelegd.

Het lid van het Team Security legt vast:

- Naam van de melder;
- De contactpersoon van Vanboxtel voor de melding;
- Datum en tijd van de melding;
- Aard van de inbreuk en risico op verlies of onrechtmatig gebruik van de gegevens;
- Welke persoonsgegevens vallen onder de melding;
- Om welk (geschat) aantal gegevensrecords het gaat;
- Welke personen betrokken zijn bij de melding;
- Welke maatregelen zijn of worden getroffen door de melder;
- Welke gevolgen er zijn volgens de melder voor de betrokkenen.

Ook buiten kantoortijden, in het weekend en tijdens feestdagen wordt de melding gedaan bij het Team Security.

Analyse

Het lid van het Team Datalekken waarbij de melding gedaan wordt, roept met hoge prioriteit het gehele Team Security en een minimaal één lid van de directie (digitaal) bij elkaar.

Het Team Datalekken:

- bespreekt de gegevens die tot dusverre zijn vastgelegd bij het aannemen van de melding;
- beoordeelt of van de inbreuk redelijkerwijs kan worden aangenomen dat de inbreuk leidt tot aanmerkelijk risico op verlies of onrechtmatige verwerking van persoonsgegevens;
- bepaalt eventuele noodzakelijke vervolgacties met betrekking tot het datalek (lek dichten, toegang tot informatie beperken en tegelijkertijd meer informatie vergaren over de eventuele indringer) en zet deze op basis van prioriteit in gang;
- informeert binnen één werkdag na signalering van het datalek de betrokken opdrachtgever(s). De opdrachtgever bepaalt vervolgens zelf of er melding van het datalek gedaan dient te worden via het Meldpunt Datalekken van de Autoriteit Persoonsgegevens. Vanboxtel verleent alle medewerking om de betrokken zo adequaat mogelijk te informeren, indien een dergelijke melding wordt gedaan.
- maakt een verslag van bovenstaande welke gedurende de verdere afhandeling van het datalek wordt aangevuld.

Het uiteindelijke verslag omvat tenminste:

- de gegevens die zijn vastgelegd bij het aannemen van de melding;
- de omvang van het datalek (bijv. aantal opdrachtgevers, aantal records per opdrachtgever enz.);
- de noodzakelijke vervolgacties met betrekking tot het datalek inclusief de status per actie;
- wat er intern gecommuniceerd wordt over het incident;
- wat er richting de betrokken opdrachtgever(s) is en nog wordt gecommuniceerd over het incident;
- of de betrokken opdrachtgever(s) wel/geen melding gaan doen of hebben gedaan bij het Meldpunt Datalekken;
- wat er extern wordt gecommuniceerd en vaststellen of de pers geïnformeerd moet worden;
- of er sprake is van schade en of in verband daarmee een verzekering ingeschakeld dient te worden;
- of er sprake is van eigen aansprakelijkheid of aansprakelijkheid van derden;
- vaststellen of er sprake is van strafrechtelijke verwijtbaarheid en gerelateerd daaraan het al dan niet doen aan aangifte.