Algemene beschrijving van de technische en organisatorische veiligheidsmaatregelen

Verwerkingsverantwoordelijke:

Naam van het bedrijf	Glaswerken Wintermans BV
Adres	Lierseweg 326 2200 Herentals
Ondernemingsnummer	0737.408.153
Telefoon	014 21 86 07
e-mail	info@wintermans.be
website	www.wintermans.be

Contactgegevens van de zaakvoerder:

Naam	Wintermans Herlinda
Adres	Lierseweg 326 2200 Herentals
Telefoon	014 21 86 07
e-mail	info@wintermans.be

Het doel van dit document is om een samenvatting te geven van alle technische en organisatorische veiligheidsmaatregelen die binnen het bedrijf zijn geïmplementeerd om de bescherming van gegevens te garanderen en de vertrouwelijkheid, integriteit en beschikbaarheid van de producten en diensten van het bedrijf te allen tijde te waarborgen.

Deze beschrijving voldoet aan de verplichtingen die voortvloeien uit artikel 32 van de Europese verordening inzake gegevensbescherming (DPR).

U kunt deze beschrijving altijd aanvullen met een cyber check die hier beschikbaar is:

https://cybercheck.ozon.io/dataprivacybox

Gratis Cyber Security Maturity Level Assessment

Identificeer hiaten in de cyberveiligheid die uw kmo blootstellen aan cyberaanvallen & data-inbreuken.

Vink de verklaringen aan die overeenkomen met de veiligheids- en organisatorische maatregelen die in uw bedrijf van kracht zijn.

Authenticatie en bevoegdverklaring

- ❑ Mechanisme voor het beheer van bevoegdverklaringen zodat alleen bevoegde personen toegang krijgen tot de persoonsgegevens
- ❑ Jaarlijkse herziening van de bevoegdverklaringen
- ❑ Gebruik van wachtwoorden en identifiers voor het authenticeren van de verbinding
- ❑ Minimumregels voor wachtwoorden
- ❑ Regelmatig wijzigen van wachtwoorden
- ❑ Gebruik van een unieke login per gebruiker
- ❑ Gebruik van een wachtwoord historiek zodat wachtwoorden niet opnieuw kunnen worden gebruikt
- ❑ Database van gehashte of versleutelde wachtwoorden
- ❑ Beperking van het aantal pogingen om toegang te krijgen tot een account
- ❑ Gebruik van beveiligingsvragen, codes, tokens, pincodes om de veiligheid van een deel van het netwerk of systeem te versterken
- ❑ Invoering van een proces voor de toewijzing, het beheer en de intrekking van toegang tot de gegevens
- ❑ Bewaren van een lijst met gebruikers van de gegevens
- ❑ Schrappen van inactieve gebruikers en verouderde toegangsmachtigingen
- ❑ De verwerking verantwoordelijke gebruikt een dubbele authenticatie
- ❑ Toewijzing van administratieve voorrechten uitsluitend op verzoek

- ❑ Andere, verduidelijken

Interne organisatie

- ❑ De veiligheidsverantwoordelijke maakt deel uit van het directieteam
- ❑ Andere, verduidelijken:

Intern beleid en procedures

- ❑ Bestaan van interne normen of standaarden in verband met de veiligheid van de gegevens
- ❑ De normen of standaarden in verband met veiligheid hebben een dwingende normatieve basis
- ❑ Beleid voor het bewaren en wissen van persoonsgegevens
- ❑ Bestaan van duidelijk omlijnde processen om te reageren op veiligheidsincidenten
- ❑ Bestaan van duidelijk omlijnde processen om wijzigingen aan te brengen aan de netwerken en informatiesystemen
- ❑ Gebruik van middelen om de permanente vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en -diensten te garanderen
- ❑ Gebruik van middelen om de persoonsgegevens binnen een gepaste termijn opnieuw beschikbaar en toegankelijk te maken bij een fysiek of technisch incident

- ❑ Gebruik van procedures voor het regelmatig testen, analyseren en evalueren van de efficiëntie van de technische en organisatorische maatregelen om een veilige verwerking te kunnen garanderen
- ❑ De verwerking verantwoordelijke heeft een beveiligd vernietigingsbeleid ontwikkeld voor vertrouwelijke gegevens (elektronisch, op papier en op verwijderbare media)

- ❑ Andere, verduidelijken:

Aansluiting

- ❑ Automatische vergrendeling van de sessies
- ❑ Waarschuwing voor elke aansluiting, met de melding dat de systemen alleen door gemachtigd personeel mogen worden gebruikt
- ❑ Oplijsten van de toegangen tot apps, verrichtingen en aansluitingen op de apps, en gebruik van die overzichten

- ❑ Andere, verduidelijken :

Beveiliging en antivirus

- ❑ Invoeren van pseudonimisering van de persoonsgegevens
- ❑ Gebruik van een versleutelingsmethode voor het beveiligen van de gegevensoverdracht
- ❑ De toegang tot de gegevens wordt uitsluitend verschaft indien dat strikt noodzakelijk is
- ❑ De interne servers en pc's van de verwerking verantwoordelijke worden gescheiden van het internet en andere externe netwerken door middel van firewalls en/of andere middelen.
- ❑ Gebruik van intrusiedetectie systemen (IDS) of intrusion prevention system (IPS)
- ❑ Wekelijkse herziening van de veiligheidsregels en alarmsignalen
- ❑ Maandelijkse herziening van de veiligheidsregels en alarmsignalen
- ❑ Alle systemen worden beschermd door een antivirusprogramma
- ❑ De antivirus handtekeningen die worden gebruikt door de verwerking verantwoordelijke worden ten minste dagelijks bijgewerkt
- ❑ Bijwerken van de veiligheid van de besturingssystemen en applicaties voor alle systemen
- ❑ De updates vinden ten minste maandelijks plaats
- ❑ De digitale gegevens worden beschermd tegen verlies of corruptie door regelmatige back-ups die afzonderlijk worden bewaard.
- ❑ Uitvoeren van penetratietests, ten minste één keer per jaar

- ❑ Andere, verduidelijken :

Informatie en bewustmakend

- ❑ De gebruikers die toegang hebben tot de gegevens worden geïnformeerd over en bewust gemaakt van de waarde ervan met het oog op de veiligheid
- ❑ De gebruikers worden geïnformeerd over en bewust gemaakt van de interne procedures inzake gegevensbeveiliging

- ❏ De gebruikers worden opgeleid in de bescherming van persoonsgegevens

- ❏ Andere, verduidelijken :

Externe aansluiting en wifi

- ❏ Beveiliging van nomadische apparaten via geschikte systemen (interne toegangsverschaffing, VPN, enz.)
- ❏ De draadloze netwerken van de verwerkingsverantwoordelijke maken gebruik van versleutelings- en toegangsprotocollen
- ❏ Invoering van WPA2- of WPA2-PSK-protocol voor draadloze netwerken

- ❏ Andere, verduidelijken :

Mobiele apparatuur

- ❏ Wachtwoord voor mobiele apparaten
- ❏ Versleuteling van de mobiele apparaten

- ❏ Andere, verduidelijken :

Fysieke bescherming van het informaticamateriaal

- ❏ Het informaticamateriaal wordt beschermd door middel van beveiligde fysieke toegang
- ❏ De fysieke toegang tot het informaticamateriaal wordt geïnventariseerd
- ❏ Het informaticamateriaal wordt beschermd bij een stroomstoring
- ❏ Het informaticamateriaal wordt beschermd bij een overstroming

- ❏ Andere, verduidelijken :

Website

- ❏ De website van de verwerking verantwoordelijke wordt beschermd door middel van een firewall
- ❏ De front end van de website van de verwerking verantwoordelijke is gescheiden van de databases en lokale netwerken
- ❏ De website van de verwerking verantwoordelijke wordt beschermd door IDS, IPS, WAF of een andere geavanceerde beveiligingsmethode
- ❏ Uitvoeren van kwetsbaarheidsscans van de website, ten minste elk trimester
- ❏ Uitvoeren van penetratietests, ten minste één keer per jaar
- ❏ De gegevens van de verwerking verantwoordelijke zijn toegankelijk via de website
- ❏ De gevoelige delen van de website van de verwerking verantwoordelijke worden beschermd door versterkte versleuteling

- ❑ Andere, verduidelijken :

Procedure voor schending van persoonsgegevens

- ❑ Procedure voor kennisgeving in het geval van de schending van persoonsgegevens
- ❑ Andere, verduidelijken :