OPTIMALE INFORMATIEBEVEILIGING MET LINX IT SOLUTIONS EN ISMS.ONLINE

De veiligheid van onze maatschappij en economie staat door diverse ontwikkelingen steeds meer onder druk. Denk daarbij aan pandemieën en oorlogen, maar ook op het gebied van cyberdreigingen hebben organisaties te maken met steeds urgentere uitdagingen. Uit onderzoek van ISMS.online blijkt dat 90% van de organisaties het afgelopen jaar te maken heeft gehad met een cyberincident. En meer dan één op de drie (36%) bedrijven heeft in de afgelopen 12 maanden te maken gehad met een datalek (bron: State of Infosec-rapport van ISMS.online).

Met het oog op de groeiende cyberdreigingen heeft de Europese Unie eind 2022 de "Network and Information Security Directive" (NIS2) vastgesteld. De NIS2-richtlijn verplicht Europese lidstaten om hun digitale en economische weerbaarheid te versterken. Het doel van de richtlijn is maximale beperking van de digitale (cyber)risico's voor de netwerk- en informatiesystemen van organisaties.

Optimale cybersecurity en naleving van nieuwe AVG-wetgeving
Met het oog op de NIS2-richtlijn adviseert de Rijksoverheid uw organisatie om nu te starten met het optimaliseren van uw cybersecurity en de continuïteit van uw bedrijfsprocessen duurzaam te waarborgen. Hiermee beveiligt uw organisatie zich tegen bestaande cyberrisico's en verzekert u dat het beleid van uw organisatie in lijn is met de nieuwe wetgeving die volgt uit de NIS2-richtlijn. Deze zal naar verwachting eind 2024 in werking treden.

Maar hoe zorgt u ervoor dat de optimalisatie van uw cybersecuritybeleid moeiteloos en efficiënt wordt geïmplementeerd in uw organisatie? De NIS2-richtlijn zal door elk van de Europese landen worden geïmplementeerd in hun eigen nationale regelgeving. Kennis over lokale regelgeving is dus cruciaal voor een goede uitvoering. Dat vraagt om een gespecialiseerde partner met gedegen kennis van digitalisering, informatiebeveiliging en privacy. Zodat de optimalisatie van uw cybersecuritybeleid voor alle relevante onderdelen van uw organisatie gegarandeerd is.

Linx IT Solutions: uw betrouwbare lokale partner
Linx IT Solutions is een duurzame partner voor klanten op het gebied van marketingcommunicatie en e-commerce. Vanuit dat perspectief zijn privacy en internetveiligheid altijd heel belangrijk geweest. Het waarborgen van de digitale veiligheid en de bescherming van de privacy maken integraal onderdeel uit van de dienstverlening aan onze klanten en vanzelfsprekend zijn wij ISO 27001 gecertificeerd. Als reseller bieden wij u, vanuit onze expertise op het gebied van informatiebeveiliging en privacy, een hoogwaardig online platform voor informatiebeveiliging aan: **ISMS.online**.

ISMS.online: het ideale Information Security Management System
Met ISMS.online kunt u uw beleid op het gebied van cybersecurity in alle lagen van uw organisatie doelgericht en gemakkelijk optimaliseren. Linx IT Solutions kan uw organisatie helpen met de effectieve en efficiënte inrichting van een online managementsysteem voor uw informatiebeveiliging. Daarnaast kunnen wij uw organisatie ondersteunen bij het opstellen van een duurzaam cybersecuritybeleid en de implementatie ervan in dat managementsysteem. Hiermee zorgt u ervoor dat uw organisatie 100% voldoet aan de nieuwe regels binnen de AVG-wetgeving en, nu én in de toekomst, beter is voorbereid op cyberdreigingen.

In deze brochure leggen wij uit wat de NIS2-richtlijn voor uw organisatie betekent, welke verplichtingen hieruit volgen en welke maatregelen uw organisatie kan nemen om aan deze verplichtingen te voldoen. Vervolgens zetten we uiteen hoe Linx IT Solutions u kan ondersteunen om te komen tot een optimaal cybersecuritybeleid.

WELKE ORGANISATIES VALLEN ONDER DE NIS2-RICHTLIJN?

De NIS2-richtlijn richt zich op organisaties waarbij de uitval van diensten een ontwrichtende impact heeft op de economie en de samenleving, en die behoren tot de volgende sectoren:

SECTOREN BIJLAGE 1

- Energie
- Transport
- Infrastructuur financiële markt
- Gezondheidszorg
- Drinkwater
- Digitale infrastructuur
- Afvalwater
- Overheidsdiensten
- Ruimtevaart
- Beheerders van ICT-diensten
- Bankwezen

SECTOREN BIJLAGE 2

- Digitale aanbieders
- Post- en koeriersdiensten
- Afvalstoffen beheer
- Levensmiddelen
- Chemische stoffen
- Onderzoek
- Vervaardiging/ manufacturing

Onderscheid essentiële en belangrijke entiteiten

Binnen de sectoren waarop de NIS2-richtlijn zich richt wordt onderscheid gemaakt tussen 'essentiële entiteiten' en 'belangrijke entiteiten'. Essentiële entiteiten zijn organisaties waarbij de uitval van diensten een grotere ontwrichtende impact heeft op de economie en samenleving dan bij belangrijke entiteiten. Het toezicht vanuit de overheid op essentiële entiteiten is intensiever dan op belangrijke entiteiten.

Essentiële entiteiten
Essentiële entiteiten zijn met name grote organisaties die actief zijn in een sector uit bijlage I van de NIS2-richtlijn (zie tabel). 'Grote' organisaties zijn organisaties met minimaal 250 werknemers of een jaaromzet van meer dan 50 miljoen euro en een balanstotaal van meer dan 43 miljoen euro.

Belangrijke entiteiten
Dit zijn middelgrote organisaties die actief zijn in een sector uit bijlage I en middelgrote en grote organisaties die actief zijn in een sector uit bijlage II. Een 'middelgrote' organisatie is een organisatie met minimaal 50 werknemers of een jaaromzet en balanstotaal van meer dan 10 miljoen euro.

Micro- en kleinbedrijven
Micro- en kleinbedrijven vallen in principe niet onder de NIS2-richtlijn, behalve als hun dienstverlening van groot belang is voor de Nederlandse economie of maatschappij.

WAT ZIJN DE VERPLICHTINGEN VANUIT DE NIS2-RICHTLIJN VOOR UW ORGANISATIE?

Organisaties die onder de NIS2-richtlijn vallen moeten aan de volgende verplichtingen voldoen:

1. **Zorgplicht**
   De NIS2-richtlijn verplicht organisaties om zelf een risicobeoordeling uit te voeren en op basis daarvan passende maatregelen te nemen om hun diensten te waarborgen en hun netwerk- en informatiesystemen te beschermen.

2. **Meldplicht**
   De NIS2-richtlijn verplicht organisaties om incidenten binnen 24 uur te melden bij de toezichthouder. Het gaat om incidenten die de verlening van de essentiële dienst aanzienlijk (kunnen) verstoren.

3. **Registratieplicht**
   Organisaties die vallen onder de NIS2-richtlijn zijn verplicht zich te registreren. Dit zorgt voor een Europees breed beeld van het aantal entiteiten onder de NIS2-richtijn.

4. **Toezicht**
   Organisaties die onder de richtlijn vallen komen ook onder toezicht te staan, waarbij wordt gekeken naar de naleving van de verplichtingen uit de richtlijn, zoals de zorg- en meldplicht.

Welke maatregelen dient uw organisatie te treffen?

De maatregelen waartoe de NIS2-richtlijn uw organisatie verplicht zijn erop gericht om gevaren op het gebied van cybersecurity maximaal te beperken. Met als doel optimale bescherming van uw netwerk- en informatiesystemen en de fysieke omgeving van die systemen tegen incidenten.

Op grond van Artikel 21, lid 1 van de NIS2-richtlijn dient uw organisatie onder andere de volgende maatregelen te nemen:

- beleid inzake risicoanalyse en beveiliging van informatiesystemen;
- incidentenbehandeling;
- beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;
- beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie.

Het organiseren van dit beleid, dat veel overeenkomsten heeft met gedeelten uit de norm ISO 27001 betreffende het beheer van informatiebeveiliging (Information Security Management), is een essentieel onderdeel uit de NIS2-richtlijn.

Linx IT Solutions: optimale implementatie verzekerd

Het toepassen van de verplichte maatregelen vanuit de NIS2-richtlijn vraagt veel van uw organisatie. Op grond van Artikel 21, lid 1 van de NIS2-richtlijn moet u beleid ontwikkelen om de cybersecurity binnen uw organisatie te verbeteren en hiertoe moeten verantwoordelijkheden worden belegd bij verschillende medewerkers en betrokken derden. Een duurzame implementatie van het beleid vereist bovendien training van uw medewerkers en consistente monitoring op naleving.

Linx IT Solutions helpt u graag om dit proces makkelijk en efficiënt te organiseren. Hier kan een geautomatiseerde – op NIS2 toegespitste versie – van het managementsysteem van grote toegevoegde waarde zijn. Als reseller bieden wij u een online platform voor informatiebeveiliging aan: ISMS.online. Met onze pragmatische aanpak ondersteunen wij u met de inrichting van dit geautomatiseerde managementsysteem, bij het opstellen van duurzaam beleid en het implementeren daarvan in het ISMS. Ook helpen wij uw organisatie bij de ontwikkeling van een doelgericht AVG-verwerkingsregister, essentieel voor de optimalisatie van de cybersecurity van uw organisatie.

Wat is een AVG-verwerkingsregister?

Als uw organisatie persoonsgegevens verwerkt (zoals namen, geboortedatums en betaalgegevens), moet u aantonen dat u dit doet volgens de privacywetgeving, ofwel AVG. Dit doet u onder meer door een verwerkingsregister te maken, waarin u aangeeft welke persoonsgegevens u gebruikt en waarom u deze gebruikt. U noteert in het verwerkingsregister bijvoorbeeld dat u 'klantgegevens' verwerkt, zoals 'namen en emailadressen'. En u vermeldt daarbij waarvoor u deze gegevens nodig hebt.

Wanneer de Autoriteit Persoonsgegevens (AP) erom vraagt, moet u het verwerkingsregister openbaar maken. Als uw organisatie geen verwerkingsregister heeft, of dit voldoet niet aan de vereisten, kan de AP uw organisatie een boete geven. Afhankelijk van het type overtreding kan deze boete hoog oplopen.

Aan de slag

Maak het makkelijk met Linx IT Solutions en ISMS.online
Er is geen vaste vorm waaraan het AVG-verwerkingsregister moet voldoen. U kunt bijvoorbeeld kiezen voor een overzicht in Excel of een online tool zoals ISMS.online.
ISMS.online maakt het opstellen van een AVG-verwerkingsregister makkelijk en overzichtelijk. Linx IT Solutions helpt u graag bij de optimale inrichting van uw ISMS zodat u zeker weet dat uw organisatie aan alle wettelijke AVG-vereisten voldoet.

Stap 1: overzicht bedrijfsprocessen

We beginnen met het definiëren van alle bedrijfsprocessen waarbij uw organisatie persoonsgegevens verwerkt. Dit noemen we ook wel 'verwerkingsactiviteiten'. Bijvoorbeeld:

- Online verkopen
- Nieuwsbrieven verzenden
- Salarisadministratie
- Personeelsdossier

Stap 2: beschrijving verplichte onderdelen AVG-verwerkingsregister

Het verwerkingsregister kent een aantal verplichte onderdelen. Linx IT Solutions ondersteunt u bij het in kaart brengen van de verplichte onderdelen van het AVG-verwerkingsregister. Dit moet in ieder geval de volgende onderdelen bevatten:

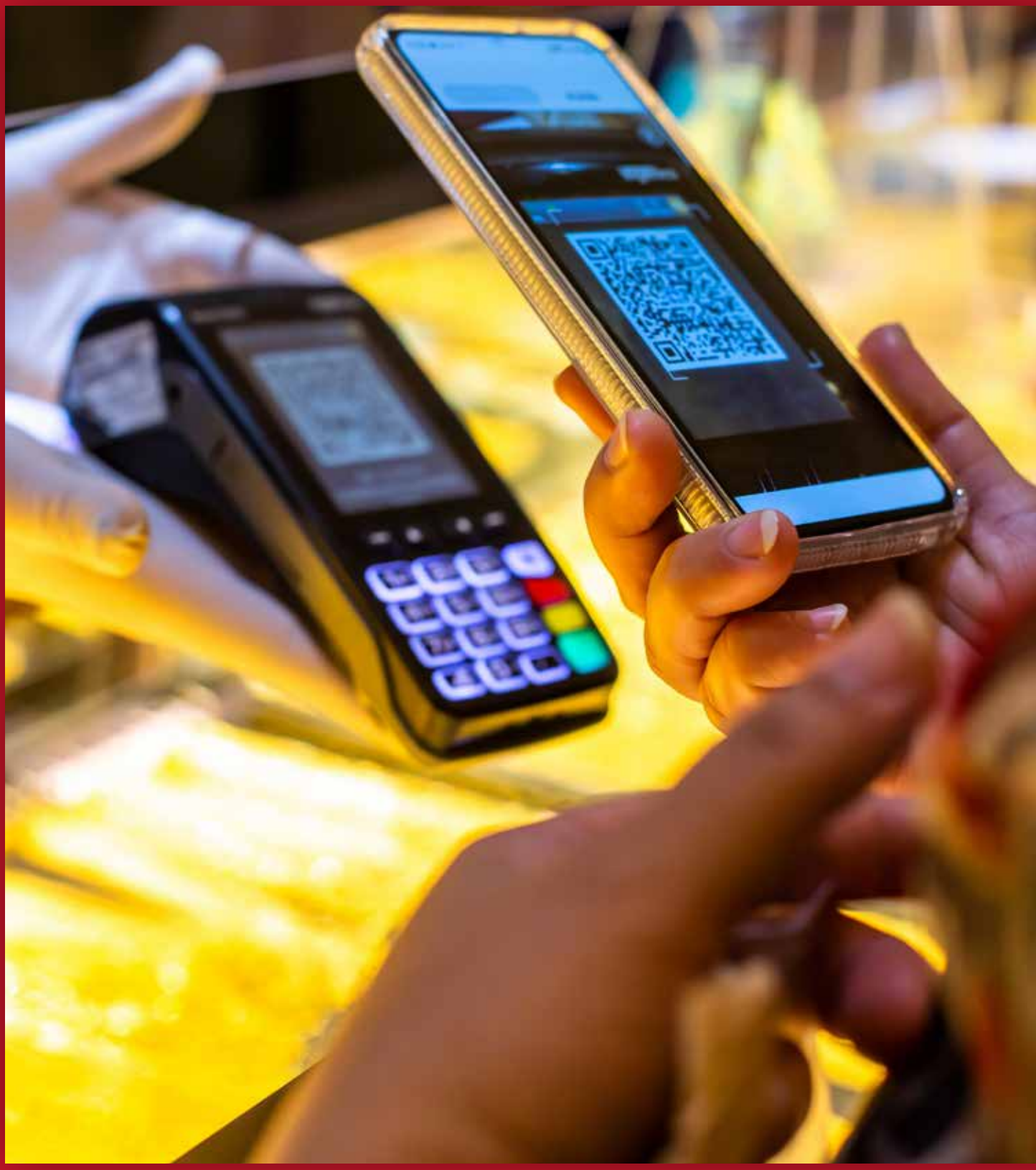
a. **Verwerkingsverantwoordelijke**
   De 'verwerkingsverantwoordelijke' is degene die bepaalt welke persoonsgegevens uw organisatie voor welk doel verzamelt. Dit kun u als ondernemer zijn of bijvoorbeeld uw besloten vennootschap.

b. **Betrokkenen**
   U beschrijft de groep personen van wie uw organisatie de gegevens verwerkt, zoals 'klanten' of 'medewerkers'.

c. **Soort persoonsgegevens**
   U vermeldt in het register welke soort persoonsgegevens u verwerkt. Bijvoorbeeld naam, adres en woonplaats, telefoonnummers of IP-adressen.

d. **Doel van de verwerking**
   Uw organisatie mag alleen persoonsgegevens gebruiken die nodig zijn voor een vooraf bepaald doel. U hebt bijvoorbeeld de adresgegevens nodig om pakketten te versturen. Het doel van de verwerking noteert u in het verwerkingsregister.

e. **Ontvangers**
   In het verwerkingsregister beschrijft u wie de persoonsgegevens ontvangt. Verstuurt u uw bestellingen bijvoorbeeld via een pakketdienst? Dan is de postleverancier een ontvanger van de persoonsgegevens die u hebt verzameld.



Verplichte onderdelen in specifieke situaties
De volgende onderdelen moet u verplicht opnemen in het verwerkingsregister als deze van toepassing zijn op de specifieke situatie van uw organisatie. Uiteraard kan Linx IT Solutions u ondersteunen met het in kaart brengen van deze verplichtingen.

a. **Beveiligingsmaatregelen**
   Als het belang van uw organisatie u hiertoe verplicht, noteert u in het verwerkingsregister met welke organisatorische en technische maatregelen u de persoonsgegevens beveiligt (bijvoorbeeld multifactor-authenticatie).

b. **Bewaartermijnen**
   Sommige persoonsgegevens moet u wettelijk een aantal jaren bewaren. Deze termijnen dient u te vermelden in het AVG-verwerkingsregister.

c. **Doorgifte naar een derde land of internationale organisatie**
   Het kan zijn dat de door uw organisatie verwerkte gegevens worden opgeslagen op een server die niet in het land staat waar uw organisatie is gevestigd. Bijvoorbeeld als u bepaalde software gebruikt voor het doen en ontvangen van betalingen. Het gebruik van dit soort software neemt u op in het AVG-verwerkingsregister.

Niet verplicht, wel verstandig
Als uw organisatie persoonsgegevens verwerkt, moet er daarvoor een juridische grondslag zijn.
Dat is een wettelijke, goede reden om persoonsgegevens te verwerken, bijvoorbeeld 'uitvoering van een overeenkomst'. Deze grondslag geldt bijvoorbeeld wanneer een klant een bestelling doet en u diens gegevens nodig hebt om de bestelling te bezorgen. Noteer in het verwerkingsregister bij elke verwerking de grondslag, dan weet u zeker dat u aan deze AVG-verplichting voldoet.

Wanneer werkt u aan het AVG-verwerkingsregister?
Zodra uw organisatie persoonsgegevens verwerkt, stelt u een verwerkingsregister op. Als u andere of nieuwe persoonsgegevens verwerkt, past u het register aan. Bijvoorbeeld wanneer uw organisatie een nieuw bedrijfsproces start, zoals het sturen van nieuwsbrieven. Zo houdt u het verwerkingsregister actueel en blijft u voldoen aan de privacywetgeving.

ONTDEK DE VOORDELEN VAN ISMS.ONLINE

Linx IT Solutions ondersteunt uw organisatie bij de ontwikkeling van een optimaal cybersecuritybeleid en doelgerichte implementatie. Voor de implementatie van een online ISMS opereert Linx als reseller voor het in het Verenigd Koninkrijk gevestigde bedrijf ISMS.online. Hun ISMS regelt meer dan 100 normen en voorschriften. De NIS2-richtlijn is er daar één van. Hiermee bent u als organisatie verzekerd van een optimale informatie-beveiliging en naleving van de AVG.

ISMS.online: ondersteuning van meer dan 100 normen en voorschriften

Ons krachtige Information Security Management System SaaS heeft alles wat u nodig hebt voor ISO 27001 en meer dan 100 andere normen:

- Compliance-software voor meer dan 100 certificeringen, normen en voorschriften, waaronder ISO 27001, ISO 27701, ISO 22301, NIST en GDPR
- Een vooraf geconfigureerd ISMS dat tot 81% vooruitgang biedt op het moment dat u zich aanmeldt
- Alle hulp die u nodig hebt met Virtual Coach, Assured Results Method, live-klantenondersteuning en een ingebouwde kennisbank

Wereldwijd vertrouwd en conform
Meer dan 1000 klanten wereldwijd, van start-ups tot wereldwijde ondernemingen, vertrouwen ISMS.online met hun compliance, zodat ze veilig kunnen schalen.

Gebruiksvriendelijk en kostenefficiënt
Kies voor de eenvoudige weg naar optimale informatiebeveiliging en naleving van de AVG met ISMS.online, het gebruiksvriendelijke online platform dat is ontworpen om u tijd, geld en moeite te besparen.

Linx IT Solutions: uw betrouwbare Nederlandse partner
Linx IT Solutions combineert expertise op het gebied van informatiebeveiliging en privacy met kennis over lokale regelgeving. Privacy by design en Security by design zijn ook de uitgangspunten voor onze eigen softwareontwikkeling en vanzelfsprekend zijn wij ISO 27001 gecertificeerd. Met Linx IT Solutions is een doelgerichte en duurzame implementatie van ISMS.online voor uw organisatie gegarandeerd.

OVER LINX IT SOLUTIONS

Linx IT Solutions is mondiaal pionier in geautomatiseerde maatwerkoplossingen. Wij werken met een eigen marketing- en fotografiemanagement-cloudplatform waarin alle functionaliteiten zijn verenigd. Onze one-stop-shop werkwijze voorkomt de noodzaak van het gebruik van verschillende systemen voor het maken van op zichzelf staande producties; er hoeft geen data te worden overgezet van het ene naar het andere systeem.

Deze technologie-infrastructuur wordt tailormade aangevuld met externe diensten die optimaal aansluiten op de interne structuur van uw organisatie. Bestaande leveranciers kunnen als procespartner op het online fotografiemanagement- en marketingplatform worden aangesloten.

Als reseller van ISMS.online bieden wij tevens een online platform voor informatiebeveiliging aan. Wij helpen met de implementatie en desgewenst met het opstellen van het benodigde beleid zodat ook uw organisatie aan de nieuwe NIS2-richtlijn voldoet!

Linx IT Solutions biedt een digitale snelweg naar online maatwerkoplossingen voor ontwikkeling, productie, beheer en exploitatie van digitale middelen. Diverse merken en retailers maken wereldwijd succesvol gebruik van onze softwareoplossingen.

LINX
IT SOLUTIONS

Linx IT Solutions B.V. • Pampuslaan 76-82 • 1382 JR Weesp • Tel. 0294 465 000