TOSHIBA
Leading Innovation

Toshiba en document-oplossingen

De Algemene Verordening Gegevensbescherming (AVG)

TOGETHER INFORMATION

INLEIDING

De hoeveelheid digitale data binnen organisaties verdubbelt iedere 12 tot 18 maanden. Big data, cloud computing en de internet of things stelt organisaties in staat enorme hoeveelheden informatie te verzamelen en te verwerken. De hoeveelheid informatie die bedrijven verwerken verspreid zich over meerdere formaten, systemen en geografieën. Zeventig procent van de informatie die een organisatie bezit is ongestructureerd en bevat persoonlijke data.

Het is voor een organisatie niet alleen belangrijk om de waarde die in data zit te verzilveren, maar ook om te voldoen aan de privacy wetgeving (GDPR/AVG) en deze data verantwoordelijk te beheren.

ALGEMENE VERORDENING GEGEVENSBESCHERMING

Wat is AVG?
De General Data Protection Regulation (GDPR) – in het Nederlands de Algemene Verordening Gegevensbescherming (AVG) – regelt bij wet dat organisaties alles in het werk moeten stellen om de data van hun klanten (consumenten, werknemers, burgers, patiënten) te beschermen. Dit heeft een grote impact op hoe organisaties persoonsgerelateerde data moeten beheren, beveiligen en hoe ze data mogen gebruiken.

Deze verordening vervangt de Wet Bescherming Persoonsgegevens uit 1995, welke niet meer aansluit op de huidige digitale wereld. De AVG is in mei 2016 in werking getreden. Van organisaties wordt verwacht dat zij vanaf die tijd hun bedrijfsvoering met de AVG in overeenstemming brengen. Zij krijgen daarvoor tot 25 mei 2018 de tijd. Op deze datum gaat het besluit AVG van kracht in alle Europese lidstaten. Daarna mag iedereen organisaties op de naleving van de AVG aanspreken. Overtreedt een organisatie de AVG, dan kan de toezichthouder een boete opleggen van maximaal twintig miljoen of vier procent van de wereldwijde omzet, mocht dat bedrag hoger uitkomen.

Particulieren kunnen zich rechtstreeks beroepen op hun bijkomende rechten inzake privacywetgeving ten aanzien van elke onderneming die persoonsgegevens verwerkt. Een kwestie van focus is uiteraard van belang, maar belangrijker dan de dreiging van boetes is hoe je omspringt met deze wetgeving. De nieuwe wetgeving biedt u als organisatie immers de kans om op een transparante en datavriendelijke manier met klanten om te gaan.

Particulieren hebben ook het recht om vergeten te worden. Het recht om vergeten te worden, ofwel vergeetrecht, is een recht voor burgers van de Europese Unie om bepaalde verouderde of onjuiste privacygevoelige informatie te laten verwijderen door verwerkers van persoonsgegevens. Deze wetgeving heeft een sterke link met de AVG wetgeving en maakt het duidelijk dat ook voor deze wetgeving controle over gegevens van belang is.

AVG BINNEN UW ORGANISATIE

AVG ook voor uw organisatie?
Met de Algemene Verordening Gegevensbescherming wil Europa bijdragen aan een hoger beschermingsniveau voor alle individuen wiens persoonsgegevens verwerkt worden.

Verwerkt u persoonsgegevens van EU-burgers voor eigen doeleinden of voor uw klanten? In beide gevallen moet u rekening houden met deze wetgeving. De definitie is zo breed dat ook gegevens die een individu indirect kunnen identificeren hieronder vallen. Veelvoorkomend zijn bijvoorbeeld de IP-adressen en informatie over het device waarop men een actie uitvoert. Deze worden op een website aan de hand van actieve cookies verzameld om de gebruiker indirect te identificeren.

Het gaat om de gegevens van personen van binnen de EU, dus uw organisatie naar een niet EU land verhuizen biedt geen antwoord op deze nieuwe wet. Ook grote organisaties zoals Google en Facebook zullen zich moeten conformeren aan deze wetgeving. Elke organisatie die zaken doet in Europa of met Europese klanten moet aan deze wetgeving voldoen.

In het kort: iedereen die persoonsgegevens verwerkt valt onder deze nieuwe wetgeving. Denk maar aan uw website ‘laat je e-mailadres achter om een whitepaper te verkrijgen’ of een winkellier die een klantenkaart aanbiedt en de gegevens hiervan verzamelt. Met de nieuwe wetgeving wordt iemand geacht zich in te schrijven om iets te ontvangen, en niet meer om zich uit te schrijven na het automatisch ontvangen van informatie.

Kortom, de wetgeving AVG zal een internationale impact hebben op hoe organisaties hun EU-gerelateerde informatie en data beheren en beschermen.

TRANSPARENCY IS KEY

De AVG verplicht ondernemingen om een transparant privacybeleid te voeren en dit beleid te verantwoorden. Daarbij geldt de stelregel ‘hoe groter de onderneming, hoe meer verantwoording’.

De meest efficiënte start om aan deze verplichting te voldoen is het opstellen van een privacy-verklaring die u online ter beschikking stelt. De privacy verklaring moet minstens het recht op inzage in de gegevens, correctie van gegevens, vergetelheid, beperken van en bezwaar tegen verwerking en het recht op gegevensopdracht bevatten. Vervolgens is een documentatie van alle stappen in de persoonsregistratie belangrijk om verantwoording te kunnen afleggen. Voor grote ondernemingen wordt het bijhouden van een register zelfs verplicht.

Duidelijk is dat u als organisatie werkprocessen moet gaan inrichten waarbij u de juiste technische, procedurele en organisatorische maatregelen neemt om ervan verzekerd te zijn dat alleen de noodzakelijke persoonlijke data voor elk specifiek doel van het proces worden verwerkt. Door uw standaard werkprocessen te automatiseren vermijdt u pro-actief het risico op datalekken en voldoet u aan de wetgeving. Bij het inrichten van uw processen moet u dan ook rekening houden met de zeven privacy beginselen die onder de AVG wetgeving vallen.

De zeven privacy beginselen van de AVG wetgeving

1. Persoonlijke data moeten eerlijk, transparant en volgens de wetgeving worden verwerkt
2. Persoonlijke data moeten voor specifieke, expliciete en legitieme doelstellingen worden verzameld en mogen niet voor andere doeleinden worden verwerkt
3. Beperk het verzamelen van persoonlijke informatie tot een minimum, zodat u het beheer hiervan beperkt
4. Persoonlijke data moeten accuraat en up-to-date zijn
5. Achterhaalde persoonsgegevens moeten worden gecorrigeerd of verwijderd
6. Persoonlijke data moeten in een versleuteld en niet te identificeren formaat worden bewaard en niet langer dan nodig
7. Persoonlijke data moeten veilig worden bewaard

CONTROLE KRIJGEN

Zakelijke documenten vertegenwoordigen een significant beveiligingsrisico als het gaat om persoonlijke data. Meer dan zestig procent van de klanteninformatie is opgeslagen in zakelijke documenten. Ook documenten die zijn opgeslagen in kasten, persoonlijke dossiers, gedeelde folders en documentmanagementsystemen vallen onder deze categorie. Omdat deze documenten hoogstwaarschijnlijk persoonlijke data bevatten, worden ook deze beschermd door de AVG wetgeving.

Het is belangrijk dat u inzicht heeft in welke persoonlijke data is gecreëerd en hoe deze wordt verwerkt, of het nu uw multifunctional betreft, de persoonlijke opslag van documenten door werknemers, of gedeelde mappen. Richt met behulp van Toshiba hard- en software uw processen zodanig in, dat u aan de wetgeving voldoet door persoonlijke data beveiligd te scannen, verwerken, beheren en op te slaan. Door de identificatie en versleuteling van persoonlijke data te automatiseren creëert u beveiligde bedrijfsprocessen, van e-mail tot print management, document opslag en workflow software die voldoet aan de AVG vereisten.

Multifunctionele systemen
Uw multifunctionele systeem is een potentieel gevaar voor bescherming van persoonlijke data. Door optimaal beheer van uw printerpark, stelt Toshiba u in staat rechten toe te wijzen aan gebruikers en authenticatie in te voeren. Hierdoor krijgt u het beheer over alle gebruikersactiviteiten op de systemen. Met rapportages kan alle input en output van de systemen worden gemonitord. De Toshiba multifunctionele systemen zijn standaard uitgerust met data encryptie, waardoor data die via deze systemen worden verwerkt versleuteld uw bedrijfsprocessen worden ingestuurd.

Screenen van content
Het grootste gevaar van bescherming van data kan liggen in het feit dat werknemers onderling of met contacten buiten uw organisatie informatie uitwisselen. De oplossingen van Toshiba helpen u documenten die via de e-mail of multifunctional worden verstuurd te screenen, zodat u ervan verzekerd bent dat er geen persoonlijke data onbeschermd wordt uitgewisseld.

Bij het screenen van documenten moet zowel de verzender als de ontvanger worden gevalideerd en de content op zoekwoorden, zinnen, patronen en bijvoorbeeld barcodes worden doorzocht. Documenten die in de gevarenzone komen moeten in quarantaine worden geplaatst voor optimale gegevensbescherming. Door een notificatie naar de verzender, leidinggevende en verantwoordelijke voor gegevensbescherming te versturen, bent u er zeker van dat er geen overtreding van wetgeving plaatsvindt.

Om aan de complexe vereisten van de AVG wetgeving te voldoen zijn het inrichten van geautomatiseerde processen een must. De eisen met betrekking tot document en data privacy en beveiliging veranderen radicaal. Maar hoe richt u voor uw organisatie het meest efficiënte digitale document management in? Toshiba helpt u uw documentmanagement op te zetten of uw huidige systeem te verbeteren.

CONCLUSIE

Toshiba kan u helpen uw persoonlijke data op een veilige en effectieve manier op te slaan, te archiveren, terug te zoeken en te verwijderen. Toshiba beschikt over de hoogste standaard oplossingen als het gaat om documenten scannen, monitoring en inrichting van document workflows en opslag en beheer van documenten. Wij helpen u graag door een analyse te maken van uw huidige bedrijfsprocessen en een aanbeveling te doen van het opzetten van uw documentmanagementsysteem of het verbeteren van uw huidige systeem.

Van veilig digitaliseren en printen tot routeren en opslaan van documenten, als organisatie blijft u verantwoordelijk te voldoen aan de AVG wetgeving. Toshiba kan u hierin ondersteunen door een totaaloplossing te bieden waarin beveiliging en monitoring van persoonlijke data wordt ingericht.

Wat biedt Toshiba?

- Inzicht in wie documenten met persoonlijke data scant, kopieert en print
- Monitoren en beveiligen van de uitwisseling van persoonlijke informatie
- Het beheren en beschermen van persoonlijke informatie in documenten
- Opslaan, archiveren, terugvinden en verwijderen van persoonlijke data zoals vereist in de AVG wetgeving
- Waarschuwingsmechnisme bij niet geautoriseerd gebruik en inbreuk op persoonlijke data
- Persoonlijke informatie veilig verwerken en opslaan Documenten die worden verwerkt via smart devices, per e-mail of op de multifunctional (printen en kopiëren) kunnen worden gecontroleerd op persoonlijke data. Wanneer persoonlijke data wordt geïdentificeerd, kan deze data automatisch worden geredigeerd om de beveiliging van het document en de klanteninformatie te waarborgen. De data kunnen vervolgens via een beveiligde en versleutelde workflow digitaal worden opgeslagen

MEER INFORMATIE?

Toshiba publiceert regelmatig informatie over actualisteiten rondom document- en informatieprocessen met als doel te informeren over de ontwikkelingen die binnen deze processen plaatvinden.

Neem voor meer informatie contact met ons op:

TOSHIBA TEC NETHERLANDS
Duwboot 31
3991 CD Houten
NEDERLAND

Telefoon
+31 (0)30 - 6348 600

Fax
+31 (0)30 - 6348 601

E-mail
info@toshibatec.nl

Website
www.toshibatec.nl

Together Information is Toshiba's visie over hoe organisaties data ontwikkelen, opslaan, verwerken, delen en beheren. Op een manier dat deze data efficiënt kunnen worden ingezet en bijdragen aan de kennis binnen organisaties.

Het is gebaseerd op onze overtuiging dat de meest succesvolle organisaties die organisaties zijn die informatie op de meest efficiënte manier communiceren.

Wij maken dit mogelijk door middel van een geïntegreerd portfolio van branchespecifieke oplossingen, die allemaal Toshiba´s inzet voor de toekomst weerspiegelen.