



Whitepaper

Hoe kun je veilig bestanden delen in de juridische sector?

Hoe kun je veilig bestanden delen in de juridische sector?

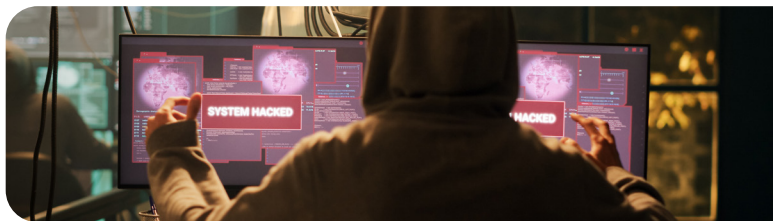
Het online delen van bestanden moet in de juridische sector uiterst veilig gebeuren vanwege de gevoelige aard van de informatie die uitgewisseld wordt. Vertrouwelijke documenten, zoals juridische dossiers, contracten en persoonlijke gegevens passeren natuurlijk dagelijks de revue. Onveilige bestandsdeling kan daarom grote gevolgen hebben, zoals datalekken en inbreuken op de privacy van cliënten. Het is dan ook van groot belang om bewust te zijn van de risico's en passende maatregelen te nemen om de veiligheid van het delen van je bestanden te garanderen.

In deze whitepaper vertellen we je daarom graag meer over hoe je veilig bestanden deelt en beroepsfouten kunt voorkomen in de juridische sector.



De risico's van onveilige bestandsdeling

Het belang van het implementeren van de juiste beveiligingsmaatregelen kan niet genoeg worden benadrukt, vooral gezien de dreiging van cybercriminaliteit en datalekken blijft toenemen. En de risico's van onveilige bestandsdeling reiken verder dan alleen financiële verliezen en reputatieschade; het kan de integriteit en vertrouwelijkheid van jouw cliëntgegevens en juridische strategieën in gevaar brengen.



Hackers en andere kwaadwillenden zijn voortdurend op zoek naar manieren om toegang te krijgen tot gevoelige informatie. Of het nu gaat om het stelen van persoonsgegevens voor identiteitsdiefstal of het compromitteren van juridische documenten voor chantage, de gevolgen kunnen verwoestend zijn voor zowel individuen als organisaties. Bovendien kunnen datalekken veroorzaakt door menselijke fouten, zoals het verzenden van vertrouwelijke documenten naar de verkeerde ontvanger, leiden tot ernstige complicaties.



Wet- en regelgeving

Naast de gevaren van externe aanvallen en menselijke fouten, is het naleven van wet- en regelgeving op het gebied van gegevensbescherming en privacy een cruciaal aspect van het werk in de juridische sector. Met de opkomst van digitale communicatie en de groeiende hoeveelheid gevoelige informatie die online wordt uitgewisseld, is het naleven van deze regels nog nooit zo belangrijk geweest.

Een van de belangrijkste wetgevingen waar juridische professionals mee te maken hebben, is de Algemene Verordening Gegevensbescherming (AVG). Deze Europese wetgeving legt strikte eisen op aan de bescherming van persoonsgegevens en de verwerking ervan. Voor advocatenkantoren en

juridische professionals betekent dit dat zij ervoor moeten zorgen dat hun praktijken voldoen aan de gestelde eisen, zoals het verkrijgen van toestemming voor het verwerken van persoonsgegevens en het implementeren van passende beveiligingsmaatregelen om de vertrouwelijkheid van deze gegevens te waarborgen.

Niet-naleving van de AVG en andere relevante wet- en regelgeving kan ernstige gevolgen hebben voor jouw kantoor, zowel financieel als reputatiegewijs. Je loopt namelijk het risico op een boete, en gerechtelijke procedures kunnen leiden tot aanzienlijke juridische kosten en reputatieschade. Bovendien kan het verlies van vertrouwen van cliënten en partners ervoor zorgen dat ze bij je weglopen.



Training en bewustwording

Een veilige manier van werken begint allemaal met het creëren van een cultuur van veiligheidsbewustzijn binnen jouw kantoor. Alle medewerkers moeten zich namelijk bewust zijn van de potentiële risico's en de noodzaak van adequate beveiligingsmaatregelen.

Training vormt een essentieel onderdeel van dit proces. Door medewerkers te voorzien van gerichte trainingen over veilige bestandsdeling, kunnen zij beter begrijpen welke praktijken en tools zij moeten gebruiken om gevoelige informatie te beschermen. Deze trainingen kunnen verschillende aspecten behandelen, waaronder het belang van het gebruik van beveiligde platforms voor bestandsdeling, het creëren van sterke wachtwoorden en het vermijden van onveilige praktijken zoals het delen van inloggegevens via e-mail.

Daarnaast is het belangrijk om medewerkers regelmatig bewust te maken van de mogelijke gevaren van onveilige bestandsdeling. Dit kan je doen door middel van interne communicatie, zoals nieuwsbrieven, memo's en workshops, waarin recente voorbeelden van datalekken worden besproken en tips over het veilig delen van bestanden worden gedeeld.



Hoe dan wel?

Om veilige bestandsoverdracht mogelijk te maken, moet je dus rekening houden met verschillende facetten en hier wil je natuurlijk niet te veel over na moeten denken. Een platform dat hier al over heeft nagedacht zou uiteraard het meest ideaal zijn.

Helaas zijn veel populaire aanbieders niet zo veilig als je zou verwachten, maar waar moet je dan op letten? Hier een aantal belangrijke punten:

1. Nederlandse hosting

Kies een platform dat gebruikmaakt van Nederlandse hosting. Dit biedt extra zekerheid omdat het onderhevig is aan de strenge Nederlandse privacywetgeving en gegevensbeschermingsnormen.

2. AVG-compatibiliteit

Zorg ervoor dat het platform voldoet aan de Algemene Verordening Gegevensbescherming (AVG) en dat het extra beveiligingsfuncties biedt, zoals Two Factor Authentication (2FA). Hiermee wordt de toegang tot het platform extra beveiligd en wordt de kans op ongeautoriseerde toegang tot je bestanden geminimaliseerd.



3. Gebruiksvriendelijkheid

Kies een platform dat gebruiksvriendelijk is en toegankelijk is via een webgebaseerde (SaaS) tool. Dit maakt het gemakkelijk voor gebruikers om bestanden te delen en te beheren, zonder dat er ingewikkelde installaties of configuraties nodig zijn.

4. Veilige data-opslag

Kies een platform dat data niet permanent op hun server opslaat. Dit verkleint namelijk de kans op datalekken omdat er geen gevoelige informatie permanent op de server wordt bewaard. In plaats daarvan moeten bestanden veilig worden overgedragen zonder dat ze achterblijven op de server.

Door deze punten in overweging te nemen bij het kiezen van een platform voor je bestandsdeling, kun je ervoor zorgen dat je vertrouwt op een veilige en betrouwbare oplossing die voldoet aan de hoogste normen voor gegevensbescherming en privacy.



mSafe voor veilige bestandsoverdracht

mSafe is zo'n veilig bestandsdeling platform en biedt een robuuste en betrouwbare oplossing voor veilige bestandsoverdracht in de juridische sector. Met standaard Two Factor Authentication (2FA) garandeert mSafe dat alleen geautoriseerde gebruikers toegang hebben tot de gedeelde bestanden, waardoor het risico op datalekken wordt geminimaliseerd.

Bovendien worden alle bestanden die via mSafe worden verstuurd automatisch gescand op virussen en malware, wat zorgt voor een extra laag van bescherming. mSafe biedt ook uitgebreide traceerbaarheid, waardoor je een volledig overzicht hebt van alle gedeelde bestanden en acties binnen je kantoor.

Door dagelijkse inspanningen op het gebied van beveiliging, encryptie en automatische malware- en virus scanning, streeft mSafe naar de hoogste normen van veiligheid en privacy. Met mSafe kun je met vertrouwen bestanden delen, wetende dat je vertrouwelijke informatie veilig is.

→ Wil je meer weten over hoe je veilig bestanden kunt delen in de juridische sector? mSafe biedt ook een workshop aan. Tijdens deze workshop nemen we jou en je collega's graag mee in hoe eenvoudig je veiliger kunt werken. Geïnteresseerd? Stuur dan een mail naar info@msafe.nl.

Maak gratis account aan

Wil je direct beginnen met het veilig delen van bestanden? Dat kan! Bij mSafe bieden we meerdere abonnementen, waaronder ook een gratis 'Go!' abonnement. Perfect voor als je soms bestanden stuurt tot 10GB per bestand. Bestanden verlopen na 7 dagen en natuurlijk is het AVG proof en wordt er gebruik gemaakt van 2-factor authenticatie.

[Maak nu een gratis account aan.](#)

