Nabestaanden checklist binnen het digitale landschap

Het leven is voor de levenden! Daarom staan we vaak niet stil bij wat het plotselinge overlijden betekent voor onze nabestaanden op digitaal vlak. Met onze sterfelijkheid of het naderende einde worden we immers niet graag geconfronteerd.

Toch is het ook in het digitale landschap belangrijk om hier aandacht aan te besteden. Het noodlot kan iedereen treffen en komt altijd onverwacht. Pas wanneer iemand er niet meer is, realiseren we ons hoezeer ons leven verweven is met verschillende digitale diensten en gegevens.

Nabestaanden hebben bijna altijd behoefte aan twee dingen:

1. De data en gegevens van de overledene, zoals foto's, documenten, contactgegevens, en e-mails.

2. Hulp bij het verwijderen van online profielen, zoals die op Facebook, Instagram, LinkedIn, enzovoort.

Waar staat jouw data en wie kan daarbij?

Voor velen van ons geldt dat onze data te vinden is op:

- Computers en laptops
- Mobiele telefoons en tablets
- Clouddiensten zoals die van:

    - Microsoft (OneDrive, Office365)
    - Google (Google Drive, Gmail)
    - Apple (iCloud)

Bij vrijwel al deze apparaten en clouddiensten is een wachtwoord en/of pincode vereist, en vaak ook een 2FA/MFA-code. Dit alles ter bevordering van de veiligheid! Echter, bij een plotseling overlijden kunnen al deze beveiligingsmaatregelen de toegang tot de data bemoeilijken of zelfs helemaal onmogelijk maken.

Dit komt doordat computers, laptops, telefoons en tablets steeds beter worden beveiligd. Data wordt steeds vaker standaard versleuteld opgeslagen, en pogingen om wachtwoorden en/of pincodes te omzeilen worden gedetecteerd en daardoor steeds moeilijker, wat kan leiden tot permanent verlies van alle data.

Gelukkig zijn er een aantal zaken die je vooraf kunt doen om het nabestaanden een stuk makkelijker te maken.

1. Breng in kaart waar je allemaal accounts hebt en welke data daar staat.

   Bijvoorbeeld: een PC is vaak gekoppeld aan een Microsoftaccount. Een Android telefoon is vaak gekoppeld aan een Googleaccount, en Mac computers en iPhones zijn vaak gekoppeld aan een Apple ID.

2. Zorg voor een lijst met actuele wachtwoorden en bewaar deze op een veilige plek, zoals een afgesloten kast of een fysiek kluisje.

   Natuurlijk is een wachtwoordkluis voor dagelijks gebruik de voorkeursmethode, maar vaak hebben nabestaanden hier geen toegang toe.

3. Maak je gebruik van 2FA/MFA? Zorg dan voor een lijst met eenmalige herstelsleutels. Hiermee kun je 2FA/MFA uitschakelen indien er om een dergelijke code wordt gevraagd en je hier geen toegang toe hebt.

4. Stel waar mogelijk noodcontacten of erfgenamen in. Bij steeds meer apparaten en cloud-accounts kun je iemand toevoegen voor noodgevallen of als contact voor de erfenis. In het geval van overlijden of ernstige ziekte kan deze aangewezen persoon bij de data. Doe dit echter voor elke dienst apart, aangezien dit voor elke dienst moet worden ingesteld.

5. Zorg voor een overlijdensakte en een akte van erfrecht. Mocht je de hulp inroepen van een gespecialiseerd bedrijf of specialist, dan mogen zij officieel alleen helpen als je deze documenten kunt overhandigen. Het omzeilen van wachtwoorden en/of pincodes mag alleen worden gedaan met toestemming van de eigenaar of de rechtmatige erfgenaam.

Extra tip: Het e-mailadres vormt in veel gevallen het middelpunt van alles. Alle wachtwoordherstelmails worden hiernaartoe gestuurd. Soms ontvang je hier ook 2FA-codes en/of links om 2FA uit te schakelen. Zorg er daarom vooral voor dat mensen toegang hebben tot het actuele wachtwoord van de mailbox.

Licentie en (her)gebruik van dit document