

Security and privacy statement

Veiligheid van data door de gehele keten geregeld en audit gereed

Als het gaat om de beveiliging en privacy van uw hosting gaat zijn er verschillende factoren die van belang zijn om te overwegen:

Geolocatie:

De fysieke servers waarop TenderIn wordt gehost, zijn gehuisvest in een locatie binnen Nederland.

Fysieke beveiliging:

Het datacenter waar de servers van TenderIn staan heeft beveiligingsmaatregelen zoals toegangscontrole, bewakingscamera's, en beveiliging 24/7 om onbevoegde toegang tot de servers te voorkomen.

Netwerkbeveiliging:

Er wordt gebruikgemaakt van firewalls en andere beveiligingsmaatregelen om de servers te beschermen tegen malware en hacking.

Data privacy:

We voldoen aan de Algemene Verordening Gegevensbescherming (AVG) van de EU om de privacy van persoonlijke gegevens te waarborgen.

Applicatiebeveiliging:

De applicatie voldoet aan de applicatieveiligheidsnormen van de ARBIT-2022 en GBIT-2020.

Backups en herstel:

Er worden dagelijks back-ups gemaakt van uw gegevens en er zijn procedures in plaats voor het herstellen van gegevens in geval van een storing of ander incident.

Certificeringen:

Het datacenter waar de servers van de TenderIn applicatie gehuisvest zijn, heeft verschillende certificeringen op het gebied van beveiliging en kwaliteit, zoals ISO 27001 en NEN 7510.

Eigen rol:

Van belangrijk is om te benadrukken dat applicatiebouwer en hostingpartij verantwoordelijk zijn voor de beveiliging van de servers en de privacy van gegevens. Het is ook belangrijk dat gebruikers zelf zorgdragen voor het veilig gebruik van de gegevens en het naleven van de relevante wet- en regelgeving.