Technische en organisatorische maatregelen

Rekening houdend met de stand van de techniek, uitvoeringskosten, alsook met de aard, omvang, context, verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treft ista passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

a) De pseudonimisering en versleuteling van persoonsgegevens

- De verwerking van persoonsgegevens wordt op zodanige wijze uitgevoerd dat de gegevens in de verschillende systemen niet zonder aanvullende informatie aan een specifieke betrokkene kunnen worden toegerekend, wanneer dit mogelijk en nuttig is.

b) Het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;

Vertrouwelijkheid

Fysieke toegangsbeveiliging

- Fysieke beperkingen op ongeoorloofde toegang tot het kantoor en haar datacenters
- Machtigingscontrole van de toegang tot gevoelige delen van datacenters door middel van ID-kaartcontrole en vergelijking met lijsten van geautoriseerde personen
- Fysieke en organisatorische veiligheidsmaatregelen zijn geïmplementeerd voor niet-openbare ruimtes
- Geïmplementeerde inbraakbeveiligingsmaatregelen (videobewaking, deurbeveiliging, alarmsysteem met veiligheidsdienst)

Logische toegangsbeveiliging

- Toegang tot systemen is alleen mogelijk met individuele gebruikersnamen en wachtwoorden
- Toegang tot de systemen is alleen mogelijk voor een bepaalde groep bevoegde personen
- Toegangsrechten worden toegekend volgens een gedefinieerd goedkeuringsproces
- De gebruikersaanmeldingen en de respectievelijke tijden worden gelogd
- Autorisatiecontroles worden uitgevoerd op basis van een autorisatieconcept
- De autorisatietoewijzing is gebaseerd op het principe van "need-to-know"
- Persoonlijke gegevens kunnen alleen worden gelezen, gekopieerd, gewijzigd of verwijderd in het kader van het autorisatieconcept
- Het gebruik van continu bijgewerkte virusbeschermingssoftware is technisch verzekerd
- Inkomend e-mailverkeer wordt gescand op virussen en spam door een centraal antivirus en anti-spam filtersysteem
- Bescherming van de IT-infrastructuur door middel van firewalls
- Wachtwoordbescherming (minstens acht cijfers, combinatie van letters, cijfers en speciale tekens, gedwongen wijziging na 90 dagen)
- Scheiding van facturering en klantstamgegevens die in het autorisatieconcept zijn geïmplementeerd
- Vastleggen van gegevenswijzigingen (logging)

Maatregelen logische systeemscheiding

- Test- en vrijgaveprocedures voor softwareproducten
- Scheiding tussen de productie en test- en ontwikkelingsomgeving
- Logische scheiding van het OTAP landschap volgens het autorisatieconcept
- Veranderingsbeheer met gedifferentieerde vrijgaveprocedure

Integriteit

Maatregelen om overdracht van gegevens te controleren

- Encryptie/gebruik van VPN-tunnels tijdens transmissies
- SSL-versleuteling voor internettoegang
- Controle van het systeemcommunicatieverkeer (centrale firewall, exclusieve WAN-verbindingen met toegangscontrole), logboekregistratie (gebruikersauthenticatie, tijd)

Maatregelen voor inputcontrole

- Plausibiliteitscontroles die aan de systeemzijde worden uitgevoerd
- Vervolgens kan worden vastgesteld of en door wie de stamgegevens van klanten in IT-systemen zijn ingevoerd, gewijzigd of verwijderd (logging).
- Autorisatieconcept

Beschikbaarheid en veerkracht

- Persoonlijke gegevens zijn altijd beschikbaar en beschermd tegen vernietiging of verlies door regelmatige back-ups van gegevens
- Data back-up concept waarbij de gegevens onsite en offsite worden bewaard
- Speciaal beveiligde datacentersecties (structurele scheiding, afzonderlijke toegangscontrolesystemen, vroegtijdige brandwaarschuwingssystemen met aansluiting op de brandweercontrolecentrale
- Brandbeveiligingsapparatuur in het kantoor
- Redundante stroomvoorzieningen
- Monitoring- en rapportagesystemen

c) Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen

    - Data recovery concept met uitwijkmogelijkheden

d) Een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking;

    - De doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking worden periodiek getoetst, rekening houdend met de stand van de techniek, uitvoeringskosten, alsook met de aard, omvang, context, verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's
    - Incidenten op het gebied van informatiebeveiliging worden gelogd en geëvalueerd

Mei 2019