Aanbeveling voor het gebruik van e-mail en Microsoft Teams in de public cloud

1. Doel

   Deze nota is een aanbeveling voor het gebruik van e-mail, het voeren van videogesprekken en het online vergaderen om de communicatie tussen instellingen, met ondernemingen, burgers en derden op een veilige manier te voeren met bescherming van de privacy van persoonsgegevens.

2. Toepassingsgebied

   De aanbeveling heeft betrekking op de Microsoft 0365 diensten “Exchange online” en “Teams” die worden aangeboden in de public cloud.

   De aanbeveling is van toepassing op alle interne medewerkers, externe medewerkers (consultants) en tijdelijke medewerkers.

   Het is wenselijk om in een volgende versie van deze aanbeveling te voorzien in een uitbreiding of aanvulling die de mailtoepassingen en samenwerkingstools van verschillende leveranciers behandelt.

3. Gegevensclassificatie

   De proceseigenaars dienen de gegevens systematisch te classificeren volgens het beleid voor gegevensclassificatie van het Federaal beleid voor informatiebeveiliging (FISP). De proceseigenaars dienen de gebruikers hierover voldoende over te informeren.

4. Risico bepaling

   Het risico dat gevoelige gegevens, zoals persoonsgegevens, onvoldoende worden beschermd en afgeschermd bij gebruik van Microsoft 0365 diensten is hoog.

   Microsoft neemt diverse veiligheidsmaatregelen om haar omgevingen af te schermen. Evenwel blijft er een risico op onrechtmatige verwerking en onrechtmatige export van gegevens.

5. Algemene aanbeveling

   De algemene aanbeveling is dat medewerkers geen persoonsgegevens uit mails, dossiers of andere bronnen mogen meedelen via e-mail of Teams.

   Dit soort van digitale verwerking moet gebeuren via beveiligde kanalen zoals de toepassingen van de instellingen of de uitwisselingsplatformen.

De aanbeveling is van toepassing voor alle communicatie tussen instellingen, met ondernemingen of met burgers.

Voor binnenkomende mail met persoonsgegevens wordt eveneens aanbevolen om geen antwoorden te versturen die persoonsgegevens bevatten en stellen we voor om in te zetten op de beveiligde kanalen.

Bijvoorbeeld: een instelling wil 1 of meerdere documenten met persoonsgevoelige gegevens bezorgen aan een andere instelling. Hiervoor kan de instelling in de eerste plaats gebruik van de applicatieve uitwisselingsmogelijkheden (bijv. API). Indien dit niet mogelijk is kan men gebruik maken van Fedsender (Belnet) waarmee deze documenten versleuteld uitgewisseld worden.

Bijvoorbeeld: Een burger vraagt via e-mail een status van zijn dossier. De instelling stuurt een antwoord via eBox. De instelling verwijst naar een portaal waar de burger deze status en details van zijn dossier kan consulteren. In deze communicatie passeert er vanuit de instelling geen enkele persoonsgevoelige data.

Bijvoorbeeld: Een instelling stelt geactualiseerde informatie over dossiers ter beschikking op een van de overheidsportalen (MyPension, MyminFin, …). Burgers en ondernemingen die dit willen consulteren en/of aanvullende gegevens bezorgen doen dit door zich aan te loggen op deze beveiligde kanalen.

6. <u>Uitzondering op de aanbeveling</u>

   In zoverre het gebruik beperkt wordt tot informatie over personen die deelnemen aan de uitwisseling van de informatie of over de personen van wie een dossier wordt behandeld en, in zoverre de uitwisseling geen andere informatie over deze individuen vrijgeeft is in volgende gevallen is het risico voor gebruik van Teams en mail aanvaardbaar:

   - Voor de uitwisseling van gegevens die onder classificatieniveau 0 van het FISP vallen.
   - Voor de uitwisseling van eenvoudige identificatie- en contactgegevens zoals:
     - Naam en Voornaam
     - Professionele adresgegevens (Gebouw, straat, nummer, bus, postcode en gemeente)
     - De organisatie waarvoor het individu zijn professionele opdracht uitvoert en de functie binnen die organisatie
     - Telefoonnummer voor professionele contactname.
     - Email adres voor professionele contactname.
     - Verwijzingen naar publiek beschikbare informatie zoals Professionele sociale media contact referenties (Facebook, Google+, LinkedIn)

   - Meta-gegevens
     - die productiegegevens bevatten (vb. titel van een mail) : deze dienen op dezelfde manier behandeld te worden als de algemene gegevens (zie hoger)
     - die nodig zijn voor het faciliteren van de technische realisatie van de uitwisseling. Dit is te vergelijken met cookies, waar we ervan uit gaan dat enkel de noodzakelijke gegevens verwerkt worden (bijvoorbeeld de participanten die deelnemen in een confcall, de ip adressen, de duurtijd van een gesprek, de

bestemmelingen van een mail bericht, de technische kwaliteit van de verbinding van de call, …);

7. Gebruik van beveiligde kanalen

   Een waaier aan beveiligde kanalen is ter beschikking van de medewerker en de instelling om de gevallen waarin e-mail of Teams niet kan gebruikt worden op te vangen.

   In bijlage is een beslissingsboom / -tabel opgenomen die de verschillende middelen aanraadt in functie van bestemmeling en ontvanger, gevoeligheid van de informatie en type van communicatie. Deze boom/tabel zal worden bijgewerkt indien de situatie het vereist.

   Voorbeelden van beveiligde kanalen zijn : Secure mail, Portal / Website, Ebox Citizen / Enterprise, beveiligde Apps (Govapp, Wallet) of uiteindelijk brievenpost.

8. Rapportage van incidenten

   Alle vermoedelijke beveiligingsincidenten met betrekking tot e-mail moeten onmiddellijk worden gemeld aan de IT-afdeling en de DPO.

9. Evaluatie en herziening

   Deze aanbeveling zal periodiek worden geëvalueerd en herzien indien nodig, om ervoor te zorgen dat het nog steeds effectief is in het beschermen van gegevens. De wijziging worden bijgehouden door middel van versiebeheer.

10. Bijkomende aanbevelingen

    Het wordt aanbevolen de medewerkers te trainen in het herkennen van cyberaanvallen en er wordt gevraagd om verdachte e-mails onmiddellijk te rapporteren.

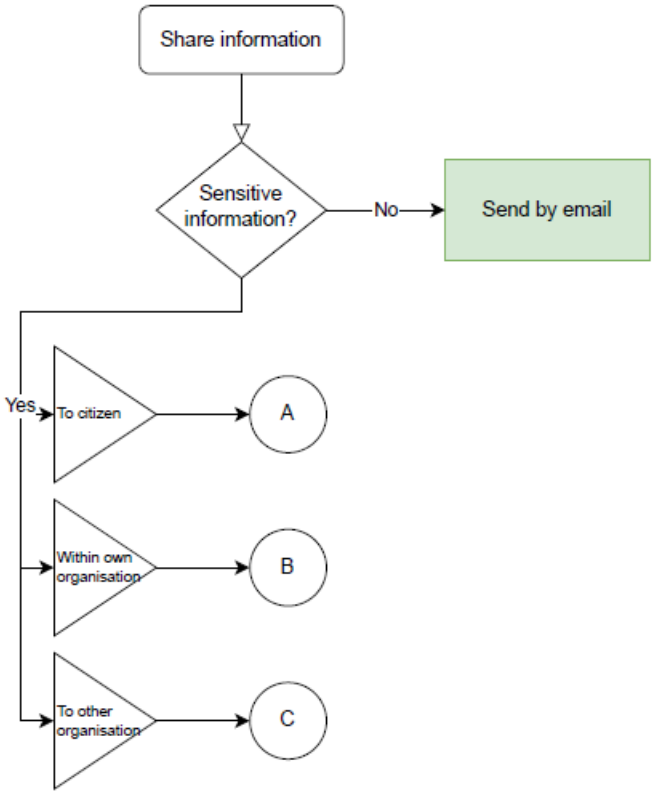
    De configuraties van de gebruikerstoestellen en de infrastructuur zal zo ingesteld worden dat er slechts een minimale set aan gebruikersgegevens wordt gedeeld. De IT-directeurs beschikken over goede praktijken om dit uit te voeren.

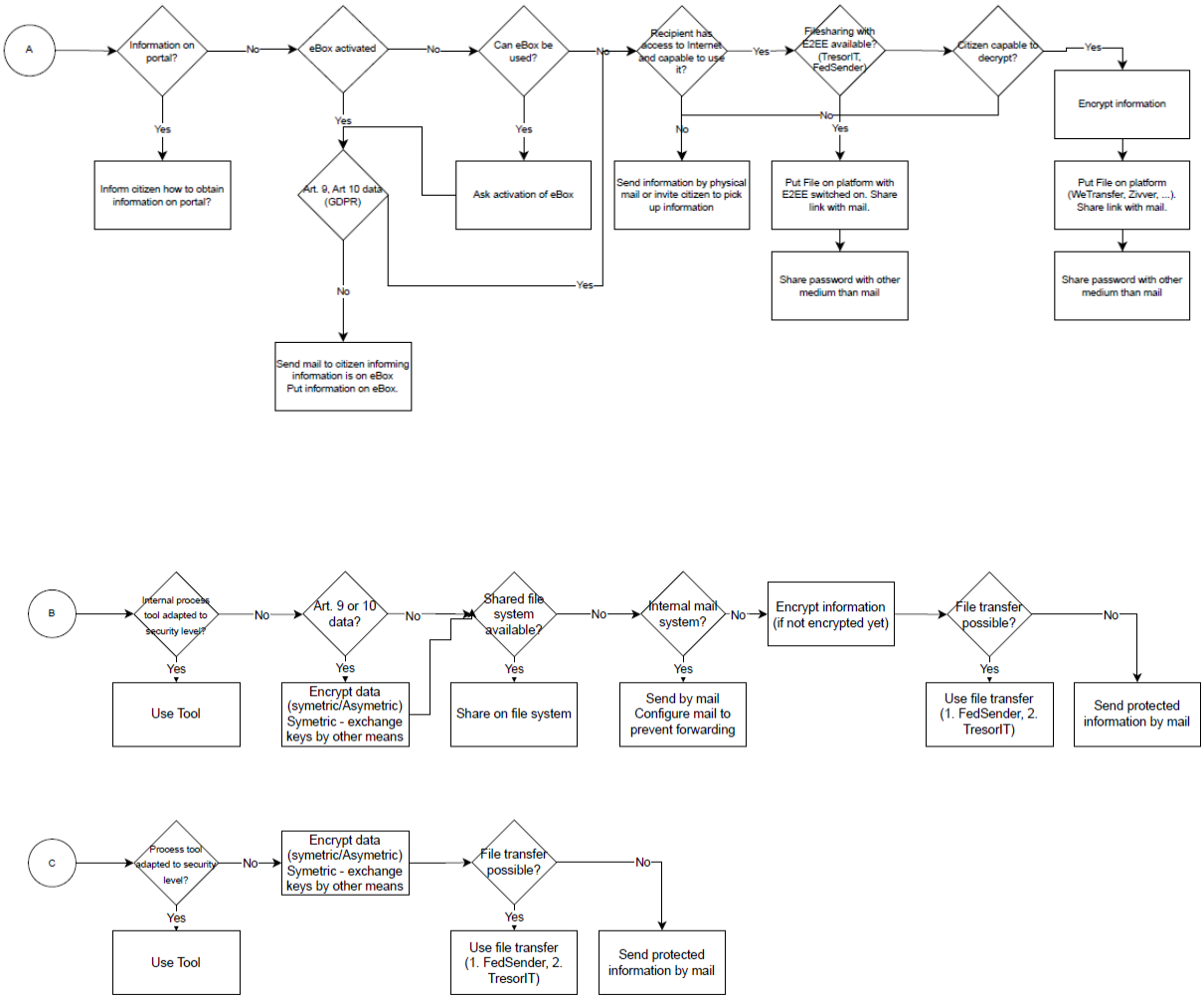
Deze aanbeveling kan worden aangepast aan de specifieke behoeften en vereisten van uw instelling. Het is belangrijk om regelmatig bewustwordingscampagnes en trainingen over deze aanbeveling te organiseren om ervoor te zorgen dat alle gebruikers op de hoogte zijn en zich eraan houden.

Het interne gebruik van mail en Teams kan sedert lange tijd zijn ingeburgerd zijn, in het bijzonder bij overheidsinstellingen die bijvoorbeeld (burger)dossiers beheren. Daarom wordt het aangeraden om een roadmap te maken om op termijn tegemoet te kunnen komen aan deze aanbevelingen en/of uitzonderlijk bepaalde risco's en hun impact in kaart te brengen en deze al dan niet te accepteren (risk appetite).

Bijlagen

Om de instellingen te ondersteunen in het bepalen van de middelen om informatie te delen zal een beslissingsboom / -tabel opgesteld en onderhouden worden die de verschillende middelen aanraadt in functie van bestemmeling en ontvanger, gevoeligheid van de informatie en type van communicatie.





Noot: Art. 9 en 10 betreft gevoelige persoonsgegevens zoals medische gegevens of rechterlijke veroordelingen. Vanwege het risico voor de betrokkene wanneer deze informatie ontsloten wordt, dient deze extra beschermd te worden.