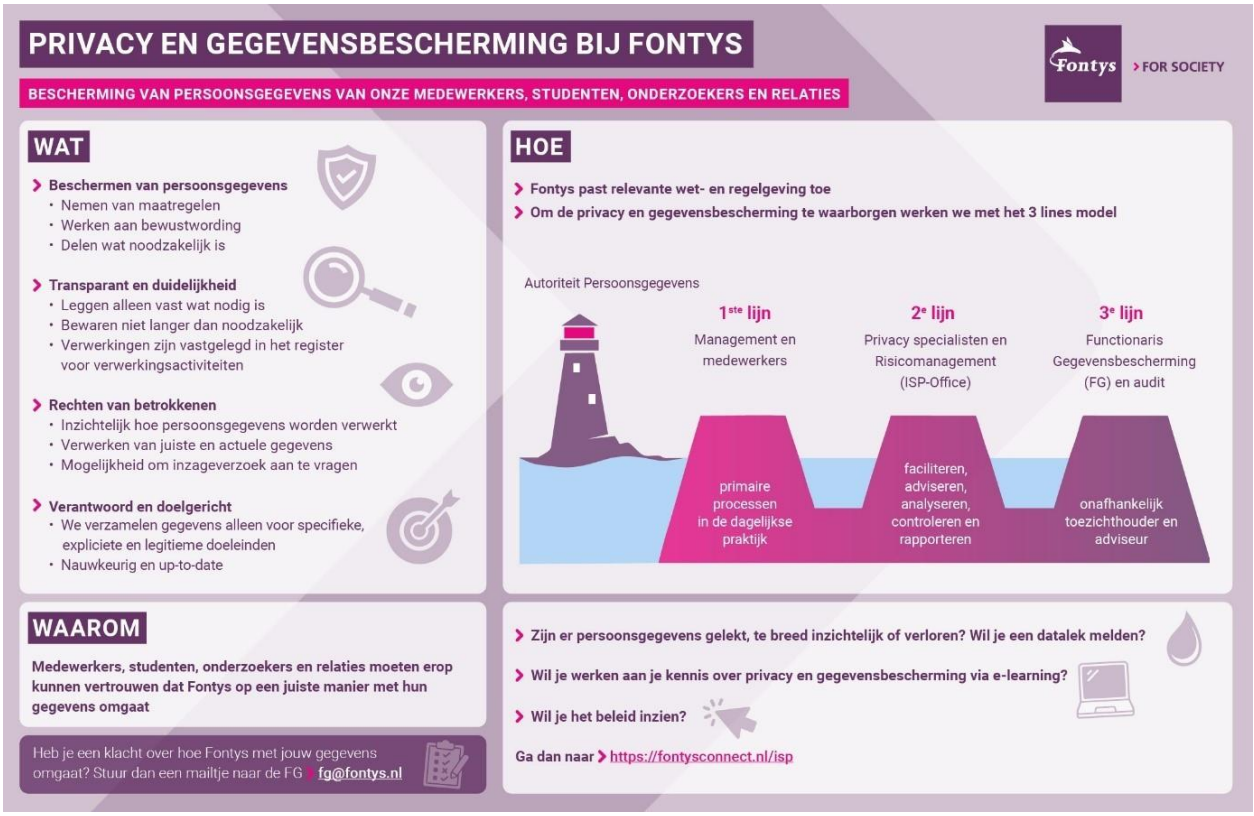
Bijlage 2: Privacy- en Securityarchitectuur

Een goed doordachte privacy- en securityarchitectuur is essentieel om gegevens te beschermen, te voldoen aan wet- en regelgeving (zoals de AVG), en risico's zoals datalekken en ongeautoriseerde toegang te minimaliseren.

Privacy architectuur

Voor elk project moet een privacytoets worden uitgevoerd. Als hieruit blijkt dat de gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor betrokkenen, moet aanvullend een DPIA (Data Protection Impact Assessment) proces worden gestart. Het ISP-Office maakt voor de registratie van de privacytoets en DPIA gebruik van Base27 (PIMS Privacy Information Management Systeem).

Daarnaast moet aan de privacyarchitectuurprincipes worden voldaan zoals deze staan beschreven in het document "Privacybeleid en regeling Fontys Hogeschool". Onderstaande afbeelding geeft een algemeen overzicht van dit privacy beleid.



Bij de privacytoets worden alle Fontys privacyprincipes doorlopen. Deze privacyprincipes zijn gebaseerd op de (beginselen van de) AVG (Algemene Verordening Gegevensbescherming) en het Fontys beleid. Een eis/verplichting (wettelijk) is dat een verwerkersovereenkomst wordt afgesloten met de leverancier om de IB&P aspecten te borgen als ketenverantwoordelijke/verwerkingsverantwoordelijke. Het ISP-Office maakt voor de registratie van de privacytoets en DPIA gebruik van een Privacy Information Management Systeem (PIMS). De uitkomsten hiervan moeten in de Solution architectuur worden opgenomen.

Wanneer een leverancier van Fontys of andere derde partij persoonsgegevens verwerkt namens of in opdracht van Fontys, is een verwerkersovereenkomst verplicht.

Privacy architectuur van IST naar SOLL

- Het uitvoeren van een privacytoets. De hierin onderkende risico's en maatregelen zijn leidend voor de verandering.
- Eventueel is het verplicht een DPIA uit te voeren (o.b.v. de resultaten privacytoets). De hierin onderkende risico's en maatregelen zijn leidend voor de verandering.
- Er moet een verwerkersovereenkomst worden afgesloten met de leverancier.
- Er mag niet worden getest met persoonsgegevens in een productie-omgeving.

Security architectuur

Voor elk project wordt een risicoanalyse uitgevoerd. De risicoanalyse wordt uitgevoerd door middel van het invullen van een security-toets in het Fontys ISMS (Information Security Management Systeem) van het ISP-office. De aanvrager vult eventueel samen met een IM-er / ISP-contactpersoon een gereedstaande lege security-toets in, bestaande uit meerdere informatiebeveiligingsgerelateerde vragen. Vervolgens worden deze antwoorden door het ISP-Office (security officer) beoordeeld en geeft deze een advies (goedkeuring / afkeuring). Een deel van de vragen is afgeleid van bestaande door Fontys ISP-Office gebruikte normen. Deze zijn voornamelijk vanuit SURF opgesteld, zie voor een overzicht hieronder. Daarnaast wordt in de security-toets ingegaan op eigenaarschap van de oplossing, applicatie, informatiesysteem en/of data. De uitkomst wordt in de Solution architectuur opgenomen.

De Fontys Security principes zoals gecommuniceerd in Bizzdesign zijn leidend voor dit project. Onder andere geldt hiervoor:

- De leverancier moet voldoen aan informatiebeveiliging, met name de onderdelen die van toepassing zijn in leveranciersrelaties (o.a. ketenbeheer):
    - SURF juridisch normenkader (cloud)services (inclusief bijlagen)
    - SURF normenkader IB HO (IB hoger onderwijs)
    - SURF toetsingskader IB HO obv het NBA model. (hierop zijn 5 volwassenheidsniveaus te onderscheiden). De verwachte norm van volwassenheid is een 3.
    - SURF Security Baseline
- In de leveranciersovereenkomst moeten de volgende beveiligingsaspecten zijn opgenomen:
    - Beheer van de dienstverlening o.a*:
        - Inrichting en werken volgens de principes: Security-by-design, en Security-by-default.
        - Autorisaties (goed en veilig proces, volgens need-to-know principe).
        - Adequaat patchmanagement, vulnerability management.
        - Beheer van wijzigingen, omgaan met problemen (problem management) en andere (ITIL) beheersprocessen.
        - Screening van personeel welke toegang kan krijgen tot onze applicatie/data, Opleiding/training van personeel inzake security/privacy.
        - Bij inzet van onderaannemers / subleveranciers: zorgdragen dat ook zij aan deze voorwaarden en eisen voldoen.
        - Direct melden van een ernstig security incident bij de Servicedesk IT.
        - Meewerken aan troubleshooting en snel dichten van security lekken.
        - Implementatie en beheer van security tools, zoals virusscanning, bescherming van apparatuur (zoals Defender).
    - Logging, monitoring en beoordeling o.a.
        - EU SCC = Standard Contractual Clauses, indien gegevens buiten de EER worden verwerkt.
        - Assurance (met o.a uit rapportage verkregen aantoonbare zekerheid).
        - Inzage in uitkomsten recente/periodieke penetratietest en ondernomen verbetermaatregelen.
        - Recht op audit door opdrachtgever danwel in inzage in audit door derde.
- De webapplicatie moet voldoen aan security- en privacy-eisen:

- Security: De mate waarin de beveiliging van de website is ingeregeld kan worden getest door de url van de website te controleren met https://www.ssllabbs.com. Uit het rapport blijkt welke kwetsbaarheden er gevonden zijn. Het rapportcijfer geeft een indicatie over het algemene beeld hoe goed de website is beveiligd. De leverancier wordt geacht de genoemde tekortkomingen vooraf op te lossen en vervolgens de test opnieuw te draaien. Indien aan bepaalde eisen (nog) niet voldaan is of kan worden dient hiervoor een grondige motivatie te worden overlegd.
- Privacy: Zeker indien er persoonsgegevens worden verwerkt, is de AVG wetgeving van kracht en zijn de daarin opgenomen eisen van toepassing. Dit betekent Privacy-by-Design en Privacy-by-default. Andere belangrijke zaken zijn o.a. (niet uitputtend): er moet een grondslag zijn om data te mogen verwerken, dataminimalisatie, verwerkersovereenkomst tussen leverancier-opdrachtgever, rechten van betrokkenen moeten ingevuld zijn, afspraken over melden van datalekken etc.

(* Deze opsomming is niet allesomvattend. Het zijn aspecten die o.a. uit de bovengenoemde SURF documenten worden benoemd. De documenten zelf en hun bijlagen beschrijven meer in detail wat de eisen inhouden.)

Security architectuur van IST naar SOLL

- Er moet een risicoanalyse worden uitgevoerd. De hierin onderkende risico's en maatregelen zijn leidend voor de verandering.
- De leverancier moet aantoonbaar voldoen aan de eisen van informatiebeveiliging en in de leveranciersovereenkomst zijn de beveiligingsaspecten opgenomen.
- Het informatiesysteem en data worden geclassificeerd middels een zogeheten BIV-classificatie. De daaruit voortvloeiden maatregelen dienen geïmplementeerd te worden.