Mededeling van Accountability

Avetica B.V.

Verantwoording van Avetica aan betrokkenen over het voldoen aan wet- en regelgeving op het gebied van privacy & informatiebeveiliging.

e-learning bereikbaar maken

(en houden)

versie 1.0 | maart 2018

Colofon

Deze Mededeling of Accountability is eigendom van:

Avetica B.V.
Sportlaan 3d
3299 XG Maasdam
088-66 44 800
info@avetica.nl
Kvk: 52832147

Deze Mededeling of Accountability is samengesteld voor klanten, medewerkers, stakeholders en belangstellenden. Het doel is om verantwoordelijkheid af te leggen over de effectiviteit van de maatregelen voor het beschermen van de persoonsgegevens van (afgeleide) klanten, medewerkers en stakeholders.

Index van wijzigingen

Onderstaande tabel geeft een overzicht van de wijziging vanaf versie 1.0.

Hoofdstuk / paragraaf	Omschrijving	Aangebracht in versie

Begrippen

In onderstaande tabel geeft een toelichting op specifieke begrippen en afkortingen.

Begrip	Toelichting
Functionaris Gegevensbescherming	Eén medewerkers van Avetica heeft de functie van (aspirant) Functionaris Gegevensbescherming.
aFG	aspirant Functionaris Gegevensbescherming.

Inhoudsopgave

Colofon 2
Index van wijzigingen 2
Begrippen 2
Inhoudsopgave 3

1. Context van Avetica 4

2. Mededeling van de directie 6

3. Mededeling Functionaris gegevensbescherming 6

4. Mededeling Internal Auditor 7

5. Vastleggen persoonsgegevens 9

6. Privacy framework 10
6.1 Verantwoording 11
6.2 Beleid 11
6.3 Awareness 12
6.4 Beoordelen van informatieveiligheidsrisico's 13
6.5 Analyse van datalekken en beveiligingsincidenten 13
6.6 Actief upgradebeleid Moodle 13
6.7 Beveiligde verbindingen 13
6.8 Tools 14

7. Ambitie voor 2018 15

1. Context van Avetica

Context van de dienstverlening

Tijdens het lezen van deze Mededeling van Accountability is het van belang om de context van de dienstverlening en daarmee ook de verwerking van persoonsgegevens duidelijk voor ogen te hebben. De core-business van Avetica is dienstverlening op het gebied van online leermanagementsystemen. Met een leermanagement kan e-learning aangeboden worden zodat een organisatie onderwijs via het internet kan aanbieden aan haar klanten en/of medewerkers. Docenten, cursusontwikkelaar, managers en sitebeheerders kunnen de leerresultaten van de gebruikers inzien om het leerproces te volgen en eventueel bij te sturen.
Avetica maakt gebruikt van Moodle als leermanagementsysteem. Dit is wereldwijd het meest gebruikte open source leermanagement. Avetica is afhankelijk van de (door)ontwikkeling van dit leermanagementsysteem.
De dienstverlening met Moodle bestaat uit hosting, support, training, advies, maatwerkontwikkeling en contentontwikkeling.

Avetica verwerkt onder andere voor de eigen personeelsadministratie persoonsgegevens van haar medewerkers. Het grootste deel van de verwerking van persoonsgegevens door Avetica bevindt zich in de honderden Moodle sites. De klanten van Avetica bieden zowel intern als extern e-learning aan. Daarmee verwerkt Avetica bijvoorbeeld ook persoonsgegevens van een cursist van een opleidingsinstituut die de hosting van Moodle heeft uitbesteed aan Avetica. Dit noemen wij de afgeleide klant.

Doel Mededeling of Accountability

Avetica wil verantwoording afleggen over de realisatie van de doelstellingen van onze serviceorganisatie en het gevoerde beleid ten aanzien van de belanghebbenden. De organisatie moet transparant zijn in haar handelen en de keuzes die worden gemaakt om daar vervolgens verantwoording over af te leggen aan belanghebbenden.
In deze Mededeling van Accountability legt Avetica verantwoording af aan alle belanghebbenden over de naleving van verplichtingen vanuit wetgeving op het gebied van privacy en informatiebeveiliging. Met een Mededeling van Accountability wordt aangegeven hoe een organisatie 'in control' is en hoe de verplichtingen vanuit wetgeving worden nageleefd. Dit gebeurt op basis van al hetgeen is gedocumenteerd in de privacy & security administratie, het bewijs van effectieve werking en andere controles. Hiermee wordt een totaalbeeld van 'accountability' gegeven.

Gebruik

Privacy en informatiebeveiliging is een onderdeel van de governance & compliance van Avetica. De (aspirant) Functionaris Gegevensbescherming ziet toe op het privacybeleid van Avetica, daarbij hoort ook de toewijzing van verantwoordelijkheden, bewustwording en opleiding en de betreffende audits. De eigenaren van applicaties en de aspirant Functionaris Gegevensbescherming zorgen voor een aantoonbare continue effectieve werking van

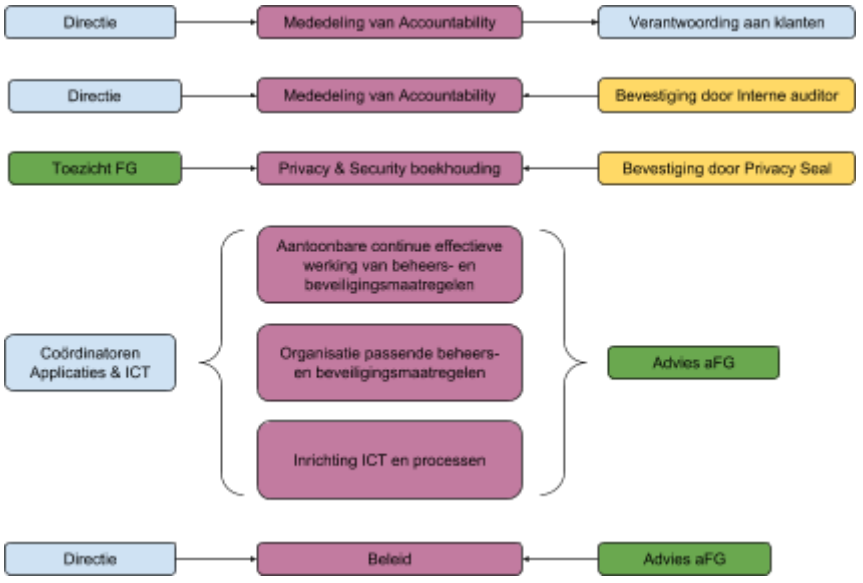
beheer en beveiligingsmaatregelen met betrekking tot onze applicaties, het organiseren van deze maatregelen en de inrichting van de IT en processen.
De Mededeling of Accountability geschreven door de aspirant Functionaris Gegevensbescherming en is bestemd voor stakeholders (belanghebbenden) zoals klanten, afgeleide klanten, medewerkers, leveranciers en andere geïnteresseerden. De controle (op aspecten) van privacy en informatiebeveiliging is onderdeel van de controle op de jaarrekening door de accountant. Daarmee is deze mededeling een jaarlijks terugkerende verantwoording.
De accountant kan de uitkomsten van de Mededeling of Accountability meenemen in het vaststellen van zijn controleverklaring.

In de 'mededeling vanuit de directie' (hoofdstuk 2) neemt de algemeen directeur en eigenaar van Avetica de volledige verantwoordelijkheid op zich voor het afleggen van de verantwoording in de Mededeling of Accountability. De directie ondertekent de Mededeling of Accountability. Omdat de functionaris voor gegevensbescherming ook de interne audit rol heeft in zijn portefeuille is ervoor gekozen om deze Mededeling of Accountability extern te laten auditen door dhr. André Biesheuvel RA van Duthler Associates.

Governance, risk management en compliance
Governance, risk management en compliance zijn ruime begrippen. Voor ons spelen de volgende elementen een grote rol:

- **Governance**: de wijze waarop onze organisatie wordt bestuurd en gecontroleerd.
- **Risk management**: het in kaart brengen en beoordelen van risico's die de doelstellingen van onze organisatie en de belangen van onze klanten raken.
- **Compliance**: werken in overeenstemming met de geldende wet- en regelgeving.

Voor Avetica ziet dit er schematisch als volgt uit:



2. Mededeling van de directie

Privacy is een fundamenteel recht dat we respecteren en omarmen maar niet kunnen afdwingen. Maar we kennen nog een ander fundamenteel recht: het recht op de bescherming van persoonsgegevens. Anders dan het recht op privacy, is dit een positief recht - daarmee wordt bedoeld dat ieder individu of betrokkene het recht heeft te verwachten dat informatie over hem met respect wordt behandeld. En ieder individu heeft daarbij het recht op inzage in zijn persoonsgegevens die over hem worden verwerkt, mag deze laten aanpassen, aanvullen of verwijderen indien dit noodzakelijk is voor het juiste inzicht over hem en in lijn is met het doel waarvoor zijn gegevens worden verwerkt. Tevens mag ieder individu, indien hij dat wenst, volledige verwijdering van zijn persoonsgegevens eisen. Het individu mag een klacht indienen bij de Autoriteit Persoonsgegevens indien hij meent dat zijn persoonsgegevens niet met respect en juist worden verwerkt en onvoldoende zijn beschermd.
Een belangrijke opdracht is dat we de persoonsgegevens van onze klanten, afgeleide klanten, medewerkers en stakeholdersbeschermen en er zorgvuldig mee omgaan. Wij hebben immers dagelijks te maken met het (geautomatiseerd) verwerken van persoonsgegevens.
Zorgvuldigheid betrachten doen we niet alleen omdat het een recht is en een wettelijke verplichting, maar ook omdat wij dat zelf erg belangrijk vinden. Dat is waar wij als Avetica voor staan. Onze klanten, afgeleide klanten en medewerkers kunnen ervan uitgaan dat wij hun recht niet schenden en dat wij inderdaad zorgvuldig met zijn of haar gegevens omgaan. En dat begint bij bewustwording bij alle betrokkenen.

Met de wijzigingen in de Wet bescherming persoonsgegevens (Wbp) en het van kracht worden van de Europese Verordening gegevensbescherming (GDPR / AVG) moest Avetica het bestaande beleid ten aanzien van privacy & gegevensbescherming verder aanscherpen.
De maatregelen die Avetica in 2017 heeft genomen op het gebied van privacy & informatiebeveiliging worden in dit document beschreven. We zijn trots dat wij weer een aantal belangrijke stappen vooruit hebben gezet.
Onze ambitie voor 2018 hebben we verwoord in hoofdstuk 6.

A.W. Vree
Directeur Avetica

3. Mededeling Functionaris gegevensbescherming

De afgelopen jaren zijn er al belangrijke stappen gezet op het gebied van beleid en awareness. De samenhang tussen alle activiteiten op het gebied van privacy en informatiebeveiliging moest nog verder geoptimaliseerd worden. Er is veel geïnvesteerd in verdere verbeteringen van het privacyvraagstuk. Een belangrijke stap hierin was behalen van het ISO 27001:2013 certificaat. De bewustwording en het draagvlak voor het verder ontwikkelen van het privacy en informatiebeveiligingsbeleid nam hierdoor snel toe.

Samen met de kwaliteitsmanager en de directeur pakten we zaken aan als het opzetten van de privacy- & security administratie, meldprocedure datalekken en het opstellen van het privacy- en informatiebeveiligingsbeleid. Een belangrijk onderdeel was ook het vorm geven van de awareness, zowel in formele bijeenkomsten of in de dagelijkse uitvoering van de werkzaamheden.

In deze Mededeling van Accountability worden aan de hand van het privacy framework alle in 2017 ondernomen acties verantwoord. Ook worden eventuele verbeterpunten en de ambitie voor het komende jaar benoemd.

D. Dubbeldam
Aspirant Functionaris Gegevensbescherming

4. Mededeling Internal Auditor

In de Internal Audit (in uitvoering uitbesteed aan drs. A.J Biesheuvel RFG RE RA van Duthler Associates) is onderzoek gedaan naar de getrouwheid van de verantwoording door de directie van Avetica, alsmede de aspirant functionaris gegevensbescherming (aFG) in de ‘Mededeling van Accountability 2018’, maart 2018.

Avetica verwerkt persoonsgegevens van haar klanten, afgeleide klanten en medewerkers. Een gedeelte van de persoonsgegevens die van de (afgeleide) klanten worden verwerkt worden omschreven als bijzondere persoonsgegevens. Het gaat met name om leerresultaten, toetsscores en (persoonlijke) reflecties die een beeld geven van de geestelijke gesteldheid van de deelnemers in de elektronische leeromgevingen.

Avetica heeft bij monde van de directie in 2017 én 2018 actief beleid ingezet en zal dat blijven doen om de organisatie naar een niveau van gegevensbescherming te brengen zodat Avetica voor mei 2018 aan voldoet aan basiseisen van de Algemene Verordening Gegevensbescherming (Avg).

Stappenplan voor invoering beleid
De directie heeft in nauw overleg met de aFG besloten het beleid in stappen te implementeren. Daartoe volgt Avetica het ambitieplan van MYOBI (https://www.myobi.eu) waarin niveaus van volwassenheid zijn opgenomen. Gekozen is om voor 2019 ambitieniveau ‘vier’ te behalen. In de ‘Mededeling van Accountability 2018’, maart 2018 is door de directie in samenspraak met de aFG verantwoording afgelegd omtrent de te bereiken doelstellingen uit het beleid en wat Avetica van die doelstellingen heeft gerealiseerd in relatie tot volwassenheidsniveau twee.

Scope van de Internal Audit
Duthler Associates heeft een intern onderzoek, lees een Internal Audit, ingesteld naar de juistheid en volledigheid van het privacy- en beveiligingsbeleid. De scope van het onderzoek is daarbij beperkt tot het vaststellen van de feiten zoals deze zijn vermeld in de hoofdstukken 2 tot en met 6 van de Mededeling van Accountability. Het doel

van het intern onderzoek is het volwassenheidsniveau vaststellen op basis waarvan eind 2018 verantwoording over de progressie kan worden afgelegd.

Uitkomsten van het Internal Audit onderzoek

Uit het onderzoek is gebleken dat Avetica het volwassenheidsniveau twee heeft behaald. Daarbij heeft Avetica zelfs al stappen genomen die na volwassenheidsniveau drie komen. Voor de vaststelling omtrent het oordeel met betrekking tot deze Mededeling van Accountability beperken wij ons echter tot de uitvoering van volwassenheidsniveau twee.

Mededeling in het kader van de uitkomsten van het Internal Audit onderzoek

Uit het onderzoek hebben wij vastgesteld dat de verantwoording van feiten in deze Mededeling van Accountability overeenkomen met de werkelijk gerealiseerde feiten. De realisatie van feiten betreffen:

- Inregelen van een managementstructuur op basis van de principes van ‘good governance’. Daarbij is het belangrijk dat de directie vanuit die good governance ook vorm geeft aan het principe Plan – Do – Check – Act zoals is aangegeven in de normenset en past bij de ISO 27001:2013 waaraan Avetica als organisatie aan voldoet;
- Aanstellen en faciliteren van een aspirant FG. De FG start met de leergang FG en na het succesvol afleggen van tentamens wordt de FG opgenomen in het FG Register, http://duthleracademy.nl/nl/fg-register;
- Instellen van een programma van Awareness voor de medewerkers van Avetica alsmede informatievoorziening aan haar klanten;
- Inregelen van de administratie bij MYOBI, de trusted third party waar Avetica zich bij heeft aangesloten en waar Avetica al haar (relevante) relaties (voornamelijk leveranciersorganisaties die uitvoering geven als bewerker van Avetica) aanmoedigt zich eveneens bij aan te sluiten om grip te krijgen op eventuele ‘gezamenlijke’ aansprakelijkheidsrisico’s. Leveranciers die zich niet willen aansluiten worden toch opgenomen in MYOBI met de duidelijke aantekening dat deze organisaties geen deel uitmaken van het controleren van de ‘gezamenlijke’ aansprakelijkheidsrisico’s;
- Inregelen van Privacy & Security Accounting. Hiertoe heeft Avetica een licentie genomen op het gebruik van SBC Managementsysteem. Van belang daarbij is dat invulling wordt gegeven aan het inrichten van de governance rondom het gebruik van SBC Managementsysteem. Daarbij doelen wij op de procedures en in te stellen interne beheersmaatregelen voor het onderhouden van deze administratie; en
- Een start is gemaakt met het kunnen gaan vaststellen van de effectieve werking van de processen. Vanuit de privacy & security administratie kan Avetica het bewijs van effectieve werking aan haar opdrachtgevers verstrekken. Deze functionaliteit zal in de komende maanden worden ingeregeld.

Aanbevelingen uit het Internal Audit onderzoek

De volgende aanbevelingen zijn van belang voor het bereiken van volwassenheidsniveau vier voor 2019:

- Onderhouden van een Plan – Do – Check – Act cyclus op het beleid zoals is ingesteld door de directie en waarbij de FG nauwgezet betrokken blijft. De informatieveiligheid, zoals is beschreven in de normenset ISO 27001:2013 (hoofdstuk 4) vormt een integraal onderdeel hiervan;
- Van leveranciers van informatiediensten het bewijs van effectieve werking opvragen en registreren van getroffen beheers- en beveiligingsmaatregelen gericht op het beschermen van persoonsgegevens zoveel mogelijke gestandaardiseerd en geautomatiseerd;
- Invulling geven aan het inrichten van de governance rondom het gebruik van het SBC Managementsysteem en ook in het gebruik van MYOBI. Daarbij doelen wij op het instellen van procedures en interne beheersmaatregelen in het gebruik van SBC Managementsysteem en MYOBI. Deze maatregelen zijn van belang om zeker te stellen dat de informatie welke in deze toepassingen worden bewaard juist, tijdig en volledig worden vastgelegd en blijven;

Met het realiseren van de interne randvoorwaarden kan Avetica meer en meer de positie van de betrokkene centraal zetten en gemakkelijker voorzien in de passieve en actieve rechten.
In het kader van het bereiken van volwassenheidsniveau vier voor 2019 adviseren wij in november 2018 wederom een Internal Audit onderzoek uit te laten voeren om zekerheid te krijgen dat de verdere implementatie van het beleid om de AVG verder te implementeren, conform het beleid wordt uitgevoerd.

Drs. A.J. Biesheuvel RFG RE RA
19 maart 2018

5. Vastleggen persoonsgegevens

Avetica verwerkt persoonsgegevens van haar klanten, afgeleide klanten, medewerkers en overiges relaties zoals leveranciers en partners. Een gedeelte van de verwerkingen van de persoonsgegevens van klanten betreffen bijzondere gegevens, namelijk leerresulaten. Daarnaast is kenmerkend dat veel persoonsgegevens een technisch karakter hebben, zoals IP-adressen en cookie. Dit heeft te maken met de hostingdienstverlening van Avetica.

Avetica verwerkt voor (afgeleide) klanten persoonsgegevens voor de volgende doelen:

- het hosten en supporten van sites waaronder online leeromgevingen, supportsystemen, bugtrackingsytemen en overige sites.
- het supporten van afgeleide klanten
- het implementeren van systemen
- het adviseren bij online leren
- het versturen van nieuwsbrieven met informatie en kennis over Moodle
- het evalueren van de dienstverlening van Avetica

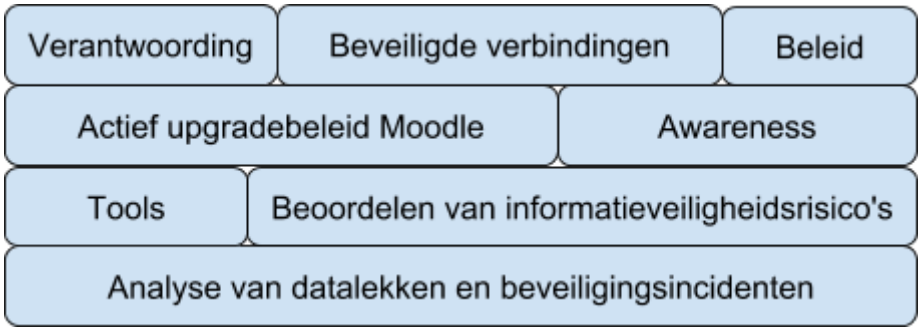
Avetica verwerkt voor haar eigen medewerkers persoonsgegevens voor de volgende doelen:

- Het behandelen van personeelszaken
- Het uitvoeren van voor de medewerkers geldende arbeidsvoorwaarden
- Het berekenen, vastleggen en betalen van salarissen, vergoedingen, belastingen, premies, uitkeringen en andere geldsommen en beloningen in natura aan of ten behoeve van medewerkers
- Het aanvragen van verklaring omtrent gedrag
- Het verstrekken van een kerstpakket
- Het afnemen van assessments bij medewerkers
- Het ontwikkelen van de medewerkers
- Het bieden van bedrijfsmedische zorg aan medewerkers
- Het geven van leiding aan de werkzaamheden van de medewerkers
- Het uitvoeren of toepassen van een (andere) wet
- Het afleggen van financiële verantwoording
- Het regelen van aanspraken op uitkeringen in verband met de beëindiging van een dienstverband
- Het verlenen van ontslag en, indien van toepassing, het regelen van uitkeringen in verband met de beëindiging van een dienstverband
- Het innen van vorderingen, waaronder inbegrepen het in handen van derden stellen van die vorderingen
- Het behandelen van geschillen
- Het uitvoeren van interne en externe controle, de bedrijfsbeveiliging en accountantscontrole
- Het doorgeven van gegevens aan KvK ten behoeve van registratie

Naast de gegevens van cliënten en medewerkers administreert Avetica ook gegevens van prospects, sollicitanten, cursisten, contractpartners, stagiaires, ZZP'ers, detachanten en ketenpartners. Van al deze verwerkingen van (persoons)gegevens zijn de doelen, specifieke gegevens en bewaartermijnen die verwerkt worden vastgelegd.

6. Privacy framework

Het privacy framework van Avetica bevat de volgende bouwstenen:



6.1 Verantwoording

De verantwoording over de stand van zaken op het gebied van privacy & informatiebeveiliging aan alle betrokkenen doet Avetica op verschillende manieren. In de Mededeling van Accountability verantwoordt Avetica zich uitvoerig over het gevoerde beleid en de ambitie voor de komende periode.
Daarnaast heeft Avetica zich op 4 december 2017 aangesloten bij Myobi. Myobi is een onafhankelijke derde die een privacy keurmerk heeft verstrekt aan Avetica. Met dit privacy keurmerk geeft Avetica op de website van Myobi en op de eigen website aan hoe zij aan de wetgeving voldoet.

6.2 Beleid

Het beleid van Avetica is verwoord in verschillende documenten waar een sterke samenhang tussen bestaat. Hieronder is per document het doel en de voortgang omschreven.

Managementsysteem voor Informatiebeveiliging

Het managementsysteem voor informatiebeveiliging beschrijft de wijze waarop Avetica continue werkt aan het informatiebeveiliging en privacy. Het management van informatiebeveiliging wordt als proces ingericht en dat houdt in dat de jaarlijkse planning en controlecyclus gebaseerd is op de Deming cyclus (Plan, Do, Check, Act). Deze aanpak geeft aan dat Avetica de kwaliteit en bereidheid in huis heeft om de processen die van invloed zijn op de informatiebeveiliging op professionele wijze te beheersen. Om aan deze doelstelling te kunnen voldoen is de organisatie doelmatig ingericht en zijn alle voor de informatiebeveiliging van belang zijnde processen overzichtelijk gerangschikt. De personeelsleden van Avetica zijn op de hoogte en vertrouwd met het informatiebeveiligingsbeleid en de daaraan gekoppelde documentatie en passen deze consequent toe. Ook zijn de personeelsleden zich bewust van het belang om volgens de eisen en wensen van klanten en andere stakeholders te werken en zijn zij op de hoogte van wettelijk opgelegde eisen en regelgeving.
Het Managementsysteem voor Informatiebeveiliging is opgesteld conform de norm ISO- 27001:2013. Via deze link kan de geldigheid van dit certificaat worden gecontroleerd.

Privacyverklaring

Avetica heeft ter bescherming van de privacy van haar klanten en medewerkers een privacyverklaring. Deze verklaring beschrijft de registratie van persoonsgegevens en de verwerking daarvan. Ook zijn de rechten van betrokkenen met betrekking tot de registratie van de persoonsgegevens opgenomen. Het gebruik van cookies op de website, opting-in en opting-out voor nieuwsbrieven, het gebruik van bezoekersstatistieken en het gebruik van gegevens van contactformulieren op de website worden ook beschreven.
Deze privacyverklaring is in 2017 opgesteld zodat het volledig aansluit bij de nieuwe wet en regelgeving.
De privacyverklaring staat op de website van Avetica, zie avetica.nl/privacyverklaring.

Informatiebeveiligingsbeleid

In 2017 is het informatiebeveiligingsbeleid opgesteld als onderdeel van de ISO 27001:2013 certificering. Dit beleid geeft richting aan de invulling van de visie en uitgangspunten die Avetica hanteert met betrekking tot informatiebeveiliging en privacyvraagstukken. Een belangrijk doel van het informatiebeveiligingsbeleid is om de kaders te stellen voor een behoorlijke en zorgvuldige verwerking van persoonsgegevens die voldoet aan de wettelijke eisen.

ICT- en internetreglement

Als onderdeel van de ISO 27001:2013 certificering is het ICT- en internetreglement opgesteld. Dit document beschrijf de regels voor hoe Avetica verwacht dat werknemers omgaan met internet en ICT-middelen binnen de arbeidsverhouding, ook in relatie tot toegang tot persoonsgegevens. Zaken als sancties en controle zijn opgenomen in dit reglement. Medewerkers worden regelmatig bewust gemaakt van de geldende gedragsregels uit dit document.

Autorisatie en authenticatie beleid

Het autorisatiebeleid geeft aan wie waarvoor toegang heeft in een bepaald applicatie en welke periodieke controle daarop plaatsvindt. Avetica beheert en monitort het autorisatiebeleid middels vaste procedures en (interne en externe) audits.
Authenticatie is het proces waarbij nagegaan wordt of iemand echt is wie hij beweert te zijn. Waar mogelijk wordt (two way) authenticatie via Google afgedwongen. Nog niet gebruikte IT-systemen ondersteunen deze authenticatiemethode. Ook zijn bepaalde applicaties alleen toegankelijk nadat een VPN connectie is opgebouwd.

6.3 Awareness

Avetica besteedt doorlopend aandacht aan de bewustwording van medewerkers op het onderwerp privacy & informatiebeveiliging. In 2017 was de aandacht in eerste instantie gericht op het verkrijgen van de ISO 27001 certificering waarbij een aantal processen en documenten samen ontwikkeld werden.
Bij bedrijfsbijeenkomsten en tijdens de vergaderingen van de verschillende teams wordt door de directie en medewerkers het onderwerp regelmatig op de agenda gezet. Daarnaast is elke mogelijkheid aangegrepen om het onderwerp op de kaart te zetten in presentaties en communicatie aan medewerkers.
Bij de ontwikkeling van software en het testen hiervan worden checklisten gebruikt waarbij veel items van deze checklisten privacy-gerelateerd zijn.

Om de awareness bij klanten te vergroten, heeft Avetica een serie artikelen geschreven op haar blog Moodlefacts.nl, namelijk:

- https://www.moodlefacts.nl/tag/moodle-privacy/
- https://www.moodlefacts.nl/tag/moodle-security/

En de komende AVG is het belangrijkste thema op het eerste Avetica Live Event wat Avetica organiseert in maart 2018.

6.4 Beoordelen van informatieveiligheidsrisico's

Periodiek worden volgens de procedures van Avetica de informatieveiligheidsrisico's in kaart gebracht volgens de gestandiseerde methode MAPGOOD. Door deze controle weten we of de informatiebeveiligingsrisico's actueel zijn en welke impact dit heeft op het informatiebeveiligingsbeleid. De uitkomst wordt besproken met de directie.

6.5 Analyse van datalekken en beveiligingsincidenten

Datalekken en beveiligingsincidenten zijn onderzocht door de aspirant Functionaris Gegevensbescherming. Avetica heeft een open cultuur waarin datalekken laagdrempelig gemeld kunnen worden. Het onderzoek van de datalekken is er primair op gericht om ervan te leren. Op basis van het onderzoek geeft de FG een advies aan de directie en zij beslist of een datalek gemeld wordt bij de Autoriteit Persoonsgegevens en/of de betrokkenen.

Geregistreerde melding 2017	Datalek	Beveiligingsincidenten
Menselijke oorzaak	0	3
Technische oorzaak	0	0
Melding door leverancier	0	0
Totaal	**0**	**3**

6.6 Actief upgradebeleid Moodle

In 2017 is actief gestuurd om een beter overzicht te krijgen van de verschillende versies van Moodle die klanten van Avetica gebruiken. Het bleek dat teveel klanten een verouderde versie draaide. Mede door een groot beveiligingslek in maart 2017 is de noodzaak duidelijk geworden om een actief upgradebeleid te voeren. Hoewel veel klanten vanwege beveiligings- en privacyperspectief de noodzaak snappen, blijkt het nog lastig te zijn om binnen bepaalde tijd alle sites te upgraden. Dit heeft mede te maken met de behorende upgradekosten en trage besluitvorming bij de klanten zelf. Avetica gaat het actief upgraden duidelijk verwoorden in de offertes en in de SLA en Algemene Voorwaarden. Avetica volgt het ondersteuningsbeleid van Moodle zelf.
In Moodle versie 3.5 die in mei 2018 uitkomt, is de AVG/GDPR volledig geimplementeerd. Avetica zal actief haar klanten op deze nieuwe versie wijzen. Voor de huidige versie 3.3 en 3.4 worden plugins uitgebracht waarmee de site voldoet aan de AVG/GDPR.

6.7 Beveiligde verbindingen

Avetica heeft de afgelopen jaren het gebruik van SSL-certificaten actief geadviseerd bij klanten. Indien een Moodle site een koppeling heeft met een extern systeem was een SSL-certificaat verplicht.
Vanaf 1 januari 2018 voert Avetica het beleid dat elke site die gehost en beheerd wordt door Avetica, is voorzien van SSL-encryptie. Met de komst van het gratis SSL-certificaat van Let's Encrypt zijn er voor de klant ook geen extra kosten aan om een beveiligde verbindingen te hebben.

6.8 Tools

Avetica zet de volgende tools in voor registratie en verantwoording van de privacy.

SBC managementsysteem

Het hart van alle activiteiten rondom privacy en informatiebeveiliging is de privacy- en security administratie (PSA). In 2017 heeft Avetica hiervoor software aangeschaft: het SBC managementsysteem. In deze software zijn in 2017 de volgende zaken vastgelegd:

- overzicht met de verbonden partijen waarmee Avetica persoonsgegevens uitwisselt
- omschrijving van alle verwerkingen met doelen, stakeholders, gegevenssets, maatregelen, processen en informatiesystemen
- verantwoording van alle door Avetica gedane activiteiten op het gebied van privacy & informatiebeveiliging
- onderzoeken die door Avetica gedaan zijn
- onderzoek van datalekken

In 2018 willen we deze administratie verder aanvullen, de volgende acties staan gepland:

- controle op de volledigheid van alle in gebruik zijnde systemen
- controle op de volledigheid van de verbonden partijen

Myobi (mind your own business)

Avetica heeft zich aangesloten bij MYOBI, een Trusted Third Party (TTP) gericht op gegevensbescherming. Avetica maakt gebruik van het privacy keurmerk van MYOBI (zie www.myobi.eu) om transparant te zijn over haar volwassenheidsniveau op het gebied van privacy en informatiebeveiliging. Door middel van volwassenheidsniveaus van het privacy keurmerk kan Avetica accountable zijn voor het niveau van gegevensbescherming dat door Avetica waargemaakt wordt. Het privacy keurmerk is onderverdeeld in zeven opeenvolgende niveaus. Door middel van een jaarlijks bestuurlijk gesprek tussen de professionals van MYOBI en

de directie wordt vastgesteld wat het op dat moment geldende niveau van de organisatie is. In januari van 2018 heeft Avetica niveau drie bereikt.

Daarnaast sluit Avetica via de TTP verwerkersovereenkomsten met partners in de keten. Door gebruik te maken van een gemeenschappelijk normenkader, datalek protocol en een mediation regeling wordt het veel eenvoudiger om verwerkersovereenkomsten af te sluiten. De aansprakelijkheden kunnen zo evenwichtiger verdeeld worden over de partijen en Avetica is voorspelbaar in het netwerk.
Tot februari 2018 heeft Avetica 20 verwerkersovereenkomsten afgesloten. We moeten met onze honderden kalnten in gesprek om een verwerkersovereenkomst af te sluiten. Hierbij lopen we tegen verschillende knelpunten aan. Vaak zijn partijen nog niet (volledig) op de hoogte van de nieuwe wetgeving en hebben ze hier nog geen visie op ontwikkeld. Andere partijen hebben zelf een verwerkingsovereenkomst opgesteld die of niet volledig is of nog gestoeld is op oude wetgeving.
Avetica heeft een plan van aanpak gemaakt met een communicatieplan om in het laatste kwartaal een forse slag te slaan met het afsluiten van verwerkersovereenkomsten.

Eén van de afspraken die gemaakt wordt in de verwerkersovereenkomst is het aantonen van de effectieve werking van de organisatorische en technische maatregelen die genomen zijn. Avetica doet dit door het ter beschikking stellen van deze Mededeling van Accountability aan alle klanten en partners. Tot nu toe hebben we nog geen bewijs van effectieve werking van klanten en partners ontvangen. In 2018 wil Avetica hier strakker op gaan sturen en klanten bewust maken van hun verantwoordelijkheid in dezen. Tevens willen we de noodzaak bespreken dat gegevensverantwoordelijken eveneens een privacy en security boekhouding voeren waardoor zij ook aantoonbaar auditable zijn aan de eisen van de Wbp en Avg.

Website

Op www.avetica.nl draagt Avetica uit dat ze een betrouwbare en voorspelbare partij is op het gebied van privacy en informatiebeveiliging. Avetica gaat het privacy keurmerk opgenomen met de hyperlink naar Myobi. Zo zien betrokkenen hoe Avetica omgaat met privacy en informatiebeveiliging.

7. Ambitie voor 2018

Voor 2018 heeft Avetica de ambitie volwassenheidsniveau 4-5 te halen.

Samengevat hebben we voor 2018 de volgende doelstellingen benoemd:

- Met alle klanten en leveranciers Verwerkersovereenkomsten afsluiten
- Google monitoringslijsten in gebruik nemen en onderdeel van de bedrijfsvoering maken
- Het overdragen van het onderhoud van de privacy & security administratie aan de functioneel applicatiebeheerders en de eigenaren van de applicaties
- Beter vastleggen van de besluitvorming over updates van systemen en het testen hiervan
- Bewijzen ontvangen dat verwerkers zich aan verplichtingen uit AVG (Wbp) houden
- Met verwerkers de noodzaak bespreken dat zij eveneens een privacy en security boekhouding voeren waardoor zij ook aantoonbaar auditable zijn aan de eisen van de AVG.
- Alle sites die Avetica host moeten supported versies zijn.
- Het implementeren van de nieuwe privacy API (release mei 2018) voor alle Moodle plugins die Avetica in eigen beheer ontwikkelt of heeft ontwikkeld.
- Alle sites die Avetica moeten voorzien zijn van SSL-certificaten. Dit geldt ook voor demo-, test en stagingssites.