ISACA
Netherlands Chapter

Welkom namens ISACA NL

Introductie & Welkom namens Kennisgroep Privacy/GDPR Comité

Fokke Jan van der Tol

IMPACT COVID-19 OP PRIVACY GOVERNANCE
SQUARE TABLE, WOENSDAG 20 MEI 2020, 19:00 – 20:00

COVID-19 maakt continuïteitsplanning en uitvoering noodzakelijk.
Welke privacy governance vragen roept dit zoal op?

Vanavond: inventarisatie, context & duiding

Opzet Square Table

- Technische regie: Stef Zelen & Dwayne Valkenburg
- Content-moderatie: Fokke Jan van der Tol
- Sprekers: Harry van den Brink, Jessica Maes, Ronald Koorn & Hans Martens
- Deelnemers graag microfoon en camera uit
- Vragen, opmerkingen etc. graag via de chat
- Email adressen zijn zichtbaar!
- PE-punten: zie uitnodigingsmail

ISACA
Netherlands Chapter

COVID & Privacy in vijf stappen

Harry van den Brink

Ergens tussen december 2019 en nu is de wereld veranderd…….

Onzekerheid door onbekendheid

ISACA Netherlands Chapter

Een virus met bigbang BCM impact

MENSEN
- Eigen personeel was ziek en niet beschikbaar, of bang, of had een zieke partner…
- Klanten/leveranciers durfden (of mochten) niet meer komen (horeca, transport ed)

PROCESSEN/PRODUCTEN/SYSTEMEN
- De 1,5 meter economie
- Van kantoorgebouw naar thuiswerkplek
- Nieuwe processen (webwinkel, bezorgservices, afstand consulten en digitaal onderwijs)

WET- en REGELGEVING continue aangepast
- Wat mag wanneer wel en niet (roadmap overheid)
- Uitwerking in brancheprotocollen (verplichting?)
- Handhaving – Overheid, Veiligheidsregio's, Gemeenten, Bedrijven, NS?, Scholen? Enz…
- Rol en visie van de AP

Ergens tussen december 2019 en nu zijn de Privacy en Security risico's veranderd…….

Nieuwe risico's, veranderde risico's

Malware ↑
Phishing ↑

Defense ↓

New threats ↑

Upscale	thuiswerken was wellicht al mogelijk. Maar meer mensen. Call centra versus directie-overleg. Capaciteit. Tooling.
Helemaal nieuwe bedrijfsprocessen	basisscholen remote onderwijs, wat mag qua (privacy) wel en niet, tentamens op Hogescholen en Universiteiten
Tooling	snel zijn nieuwe tools naar binnen gehaald. Zijn dit de juiste? (Discussie ZOOM). Maar ook: webshop-software, modules van standardpakketten
BYOD	wat betekent het dat medewerkers op eigen computers werken? Printer met pincode versus de HP voor de kleurplaten, de blauwe container ipv papiervernietigers, malware bescherming, USB poorten etc
Nieuwe (medische) taken	temperatuur meten, vragenlijsten (mondeling/schriftelijk)
Security teams	effecten van onderbezetting kritieke functies, controle logging even getemporiseerd?

Proportioneel en Consent

Hoe tijdelijk is tijdelijk?

Is er een alternatieve maatregel denkbaar om privacy schending te voorkomen

- Snel worden maatregelen met zeer verstrekkende privacy gevolgen genomen. Zijn deze proportioneel? Denk aan verplicht app installeren, opvragen telecom gegevens.
- En hoe zit het met consent? mag ik als werknemer, leverancier, klant weigeren om mijn temperatuur te laten meten?

Hoe balanceer je wettelijke eisen (waarbij de GDPR in Europa toch iets rekbaarder blijkt dan eerst gedacht), het bedrijfsbelang, gezondheid en privacy rechten?

NB: voor echte privacy liefhebbers een Walhalla: in plaats van juridische verwerkersovereenkomsten kunnen nu de wezenlijke vragen en uitgangspunten worden besproken!

Passende technische en organisatorisch maatregelen

Nieuwe risico's, veranderde risico's

ISO27701 (PIMS)

Het is nu tijd om de (privacy en security) risk registers flink op te schudden: vanaf het begin (is onze risico bereidheid veranderd?), de inventarisatie en inschattingen tot en met de getroffen en te treffen maatregelen.
Denk ook aan eventuele herstelacties: als er in de hectiek zaken zijn gebeurd die achteraf niet door de privacy beugel kunnen (DPIA), herstel die (zo mogelijk) dan netjes.

Hashtags: PDCA cyclus, risk register, privacy management system

Privacy governance

Privacy in the boardroom / CEO & COO

Never waste a good crisis!

Het is nu de tijd om 'privacy by design' echt te gaan implementeren, startend bij een goede privacy governance. Privacy raakt meer dan de juridische afdeling en de ICT organisatie.

ISACA Netherlands Chapter

Thuiswerkconcepten tijdens COVID

Jessica Maes

Impact op persoonsgegevens

- Stoppen van Covid-19 kan alleen door het meer delen van persoonsgegevens en meer monitoring" (trend in de media)
- Grenzen van de regelgeving (op meerdere fronten) verkend
- Onder druk aanpassingen in organisaties om processen te digitaliseren
- Blijf hierbij kritisch en denk in mogelijkheden, maar ook in risico’s

Thuiswerken en tools

- Gevaren en mogelijkheden van videobellen
- NCSC en AP hebben whitepapers/hulplijsten (zie site AP)

Tips:

- citrixproblematiek
- versleuteling van gegevens
- maak medewerkers bewust, denk goed na of videobellen noodzakelijk is (risicoafweging)
- verwerkersovereenkomst/voorwaarden
- verzamelen gegevens (zoals contacten/agenda's)
- gebruik van privé telefoon vs werktelefoon
- mogelijkheid tot opnemen van gesprekken of vergaderingen

- ☺ risicovoorbeeld is Avatarify (deepfaking van een celebrity)-->CEO fraude?

ISACA
Netherlands Chapter

Tracking & tracing

Ronald Koorn

Tracking & Tracing (1/3)

ISACA Netherlands Chapter
Ronald Koorn
(ISACA- Kennisgroep GDPR)

- Algemeen:
  - Allerlei ICT-middelen ingezet voor thuiswerken t.b.v. business resilience
  - Medewerkers en studenten werken vrijwel volledig thuis, soms op apparatuur van werkgever, soms – noodgedwongen – op eigen BYOD-apparatuur (of eigenlijk UMOD: Use My Own Device)
  - Diverse andere (goedbedoelde) initiatieven, o.a.:
    - Fitness/wellness-programma's: verstrekken smartbands/-watches
    - Camera's voor veiligheid
    - Kentekenherkenning (ANPR) voor parkeren, milieuzones, verzekering, e.d.
    - (IoT) sensordata voor leefbaarheid, crowd control, e.d.
  - Risico's:
    - Grootschalige (multi-mediale) gegevensverzameling: sociale & fysieke controle verschuift bij aantal organisaties naar online monitoring
    - Gebrek aan transparantie & scope creep
    - Automatische consent: vrijwilligheid vs. verplichting, maar ook sociale druk om videobellen, stappenteller, e.d. toe te passen
    - Koppelen aan social ID's & advertentienetwerken
    - Authenticatie & autorisatie
    - Indirecte herleidbaarheid / her-identificatie 'anonieme' data
    - Minderjarigen
    - Dataretentie
  - Niet louter hypothetische risico's, maar in de praktijk voorgekomen:

easyJet NHS Digital Royal Mail

Tracking & Tracing (2/3)

ISACA Netherlands Chapter
Ronald Koorn
(ISACA- Kennisgroep GDPR)

- Specifieke aspecten binnen organisaties:
  - Monitoren toetsaanslagen/screenprints
  - Protocol & instemming OR
  - Noodzaak & rol Functionaris Gegevensbescherming – Privacy Officer
  - Noodzaak DPIA / GEB
  - Online proctoring: overnemen computer, video-opname vanuit andere hoek
  - Temperatuur opnemen mag niet (zomaar) oordeelt de AP

- Specifieke aspecten in maatschappij:
  - Inzet van camerawagens (surveillance) en drones voor openbare orde
  - Wie beschikt over geolocatiedata?
  - Ontsluiten medische gegevens via Corona-opt-in
  - Toepassen van Covid-19 Alert-app
  - Telecomdata en daarmee locatiedata opvragen bij telco's en beschikbaar stellen aan GGD's en RIVM?

Tracking & Tracing (3/3)

ISACA Netherlands Chapter
Ronald Koorn
(ISACA- Kennisgroep GDPR)

- Maatregelen:
  - Privacy by Design o.b.v. DPIA
    - Privacyvriendelijk ontwerp vanaf de start
    - Transparantie
    - Mobile Device Management
    - Multi-factorauthenticatie
    - Dataminimalisatie (proportioneel / subsidiariteit)
    - Decentrale vs. centrale opslag
    - Encryptie
    - Anonimisering & Pseudonimisering
    - Invullen rechten betrokkenen
    - Bewaartermijnen

Covid & medisch-wetenschappelijk onderzoek

Hans Martens

medisch-wetenschappelijk onderzoek (clinical trials)

- Aantonen veiligheid en effectiviteit van geneesmiddelen;
- Gepseudonymiseerde gezondheidsdata;
- Kwaliteitsborging nodig, bijvoorbeeld vergelijken van brondata in het medisch dossier met de door arts verstrekte informatie (‘monitoren’);
- Wet medisch wetenschappelijk onderzoek met mensen;
- Good Clinical Practice (verklaring van Helsinki);
- Algemene verordening Gegevensbescherming;
- Verdere richtlijnen van CCMO (Centrale Commissie Mensgebonden Onderzoek).

Invloed op medisch-wetenschappelijk onderzoek (clinical trials)

- In onderzoek: verwerken medische informatie patiënten;
- Impact: geen ziekenhuisbezoek voor data controle (integriteit);
- Gevolg: andere manieren om veiligheid patiënten en data integriteit te waarborgen (‘remote monitoring’);
- Dus andere verwerking van persoonsgegevens voorlopig:
  - Sturen van kopie van (gepseudonymiseerd) medisch dossier (veelal in EU niet toegestaan door overheden);
  - On-line inzien van medisch dossier, bijvoorbeeld via video;
  - (Remote) toegang krijgen tot electronisch medisch dossier (soms al gedaan).

Invloed op medisch-wetenschappelijk onderzoek (clinical trials)

- Notice (informeren van de patient) en consent;
- Data minimizatie: alleen verwerken bij noodzaak na afweging van veiligheid patiënten en data integriteit;
- Data minimizatie: alleen gegevens die noodzakelijk zijn verwerken;
- Beveiliging van gegevens: alleen ‘veilige’ systemen gebruiken;
- Internationale transfer: vermijden (US)cloud;
- Waar nodig contracten (verwerkingsovereenkomsten) tekenen;
- Risico-assessment doen, consulteren FG;
- Training voor werknemers die techniek toepassen;
- Pseudonymizeren indien mogelijk en waar kan.

Invloed op medisch-wetenschappelijk onderzoek (clinical trials)

- Richtlijnen:
  - Centrale Commissie Mensgebonden Onderzoek: Recommendations for the conduct of clinical research at the time of restrictive measures due to the coronavirus
  - European Medicines Agency (EMA): GUIDANCE ON THE MANAGEMENT OF CLINICAL TRIALS DURING THE COVID-19 (CORONAVIRUS) PANDEMIC
  - FDA Guidance on Conduct of Clinical Trials of Medical Products during COVID-19 Public Health Emergency

ISACA Netherlands Chapter

Samenvatting: de hints en tips

Harry van den Brink

Risk based, By Design, Proportioneel en Consent, Alternatieven, Boardroom

Never waste a good crisis!

Privacy governance

ISO27701 (PIMS)

- Onder druk wordt alles vloeibaar, the show must go on: door veranderingen in mensen, processen, producten en tooling zijn nieuwe risico's ontstaan. Inventariseer en weeg af; DPIA!
- Geef meer aandacht aan 'privacy by design', het is meer dan een alinea in een projectplan;
- Pas het (privacy) risk proces aan op een meer dynamische omgeving. Ook regelgeving is niet in steen gehouwen!
- Gebruik deze situatie om 'Privacy in the Boardroom' bij de CEO/COO te versterken.

Awareness is key

Never waste a good crisis!

Communicatie en thuiswerken

- Blijf kritisch op de inzet van communicatietools: zijn er alternatieven?
- Net als bij malware en phishing: hou je medewerkers risicobewust bij het gebruik van communicatietools. Zowel van het eigen bedrijf als bij communicatie met derden.

Betrokkenheid

Never waste a good crisis!

Belang DPIA, Meer dan wet alleen

- Betrek ook medewerkers en OR direct bij de DPIA op monitoring/tracking van (online) activiteiten;
- Bekijk tracking & Tracing niet alleen vanuit AVG-vereisten, maar ook vanuit ethisch oogpunt: "het mag wettelijk, maar het deugt eigenlijk niet".

Zelfs in crisis, blijf basic privacy principes toepassen

Never waste a good crisis!

Clinical trials

- Alleen verzamelen wat nodig is (minimalisatie);
- Training van werknemers;
- Risico-assessment, begrijp hoe je proces in elkaar zit.

ISACA Netherlands Chapter

Vragen, opmerkingen, discussie en afsluiting

Allen, Fokke Jan van der Tol

SQUARE TABLE IMPACT COVID-19 OP PRIVACY GOVERNANCE

ISACA Netherlands Chapter

Content

Kennisgroep Privacy/GDPR Comité:
Hilko Batterink
Menno Borst
Harry van den Brink
Bart van Gerven
Ronald Koorn
Martin Kroonsberg
Jessica Maes
Hans Martens
Lodewijk Olthof
Fokke Jan van der Tol
Bas Wevers
Jérôme Zijderveld

Techniek

Dwayne Valkenburg & Stef Zelen