Universitair Ziekenhuis Gent

Privacy – Knowledge 2 Connect
Privacy & Biomedisch Onderzoek

23.11.2013 "LunchOntmoeting KCGG"

Ing. F. De Meyer Msc.
Vakgroep Maatschappelijke Gezondheidkunde
Onderzoeksgroep Medische Informatica & Statistiek
5K3 – Universitair Ziekenhuis – Gent
(filip.demeyer@ugent.be of filip.demeyer@uzgent.be)

Universitair Ziekenhuis Gent

Privacy - Introductie

"People, of course, are secretive and for many reasons want to appear what they call 'ordinary'. Everybody has thoughts they want to conceal, Perhaps even quite simple aspects of their lives. People have obsessions and fears and and passions which they don't admit to. I think any character is interesting and has extremes"
(Iris Murdoch)

"As long as we value liberty, we must value privacy"

Universitair Ziekenhuis Gent

Beware of privacy – security fallacies !

"Privacy can and must co-exist alongside other critical requirements: security, functionality, operational efficiency, organizational control, business processes, and usability in a "positive-sum", or doubly enabling "win-win" equation."

→ Privacy Enhancing Technologies (PET)

Privacy by design: the definitive workshop. A foreword by Ann Cavoukian.
IDIS (2010) 3:247–251 DOI 10.1007/s12394-010-0062-y

Universitair Ziekenhuis Gent


Privacy - achtergronden (simplificatie!)

- **Orwelliaanse aspecten**
  - observatie, ongecontroleerde gegevensinzameling en communicatie
  - "wat men over betrokkene weet"
  - betrokkene weet niet steeds wie wat over hem weet
  - (sterk) subjectieve impact en belang
- **Kafkaesque aspecten**
  - gebruik van gegevens voor individuele beslissingen over betrokken. → kan heel concreet zijn
  - daarom: data moet juist zijn en relevant !
  - finaliteit van verwerking moet gekend zijn
  - (DPD recital 29 bepaalt dat research data niet mogen gebruikt worden voor individuele beslissingen !)

Universitair Ziekenhuis Gent

Sidenote: EU – US Differences (Privacy)

- *EU is Romeins Recht / Napoleontische code gebied !*
- *US (en andere) zijn "common law" gebieden*
- *Verschillende uitgangspunten wat Privacy Betreft*
  - **EU: Privacy is een positief recht → regulering**
  - **Common Law: "Privacy as such niet in basiswet"**
  - **Tort law: erkenning van schade door gebrek aan privacy**
- *EU: overtreden en respecteren zijn duidelijker gereglementeerd, doch drempel tot procedures*
- *US: "litigation oriented"*
- *Verschil uit zich b.v.b. in redeneringen i.v.m privacy in wetenschappelijk onderzoek*

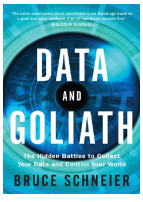
"In God we trust, all others we monitor"
-
"Collect it all, know it all, exploit it all"

Universitair Ziekenhuis Gent

"Stalker Economy"

"An entire data broker industry has sprung up around profiting from our data, and our personal information is being bought and sold without our knowledge and consent"

"There is enormous value in aggregating our data for medical research and other tasks that benefit society. We need to figure out how to collectively get that value while minimizing the harms. This is the fundamental issue..."



Data & New Technologies

Gebruik van Data in Onderzoek voor het testen van hypotheses.
Gebruik van Data voor het "opstellen" van nieuwe hypotheses ("trawling").
- ***"Big Data"-->Data en Meta-data.***

Nieuwe technologie en "anders" gebruik van bestaande technologie (& data)

- ***Geolocatie-data vanuit locatie-diensten (GPS, GLONASS,...)***
- ***Afgeleide Geolocatie data uit metadata (wifi, roaming data,BT...)***
- ***Miniatuursensoren: o.a. richting, versnelling en beweging***
- ***mHealth: zowel dedicated apps als mobiele "browsers"***
- ***Hartslag, blood gasses, pH, etc. (nanosensoren, lab on chip,...)***
- ***Analyse van gezichtsuitdrukking, stem, loop('gait'),...***
- ***mHealth: zowel dedicated apps als mobiele "browsers"***

- ***Huidige en toekomstige analysetechnieken van deze "raw data"***

*'The Fundamental problems in computer security are no longer about technology ; they're about **applying** technology'*

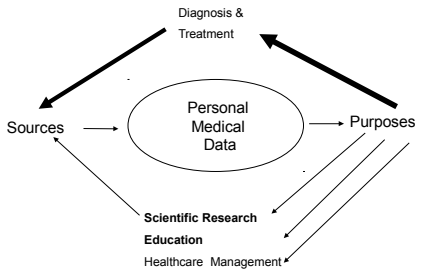
Bruce Schneier

Privacy Protection → **Data** Protection

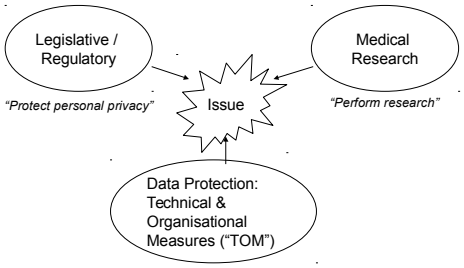
→ "Data Protectie-wetgeving
→ DPD, GDPR, WVP&KB
→ beroepsgeheim
→ sector/domeinspecifiek (e.g.GCP,MLM,...)
→ Informatica-gerelateerde wetgeving

→ "generieke" wetgeving

The Context of Personal Medical Data



Technical & Organisational Measures



"Provide protective solutions that are effective"

- **Systemen**
  - processoren, (geheugen),randapparaten, netwerk
- **Verbindingen** tussen systemen
  - 'networked' vs. lokaal, bedraad (wired),draadloos ('airgap'): wifi, BT, Zigbee, Lora,etc.
- **Data & Metadata**
  - "locatie"
    - 'on the move' (in "messaging" toestand)
    - 'statisch, opgeslagen' (magnetisch, solid state,...)
  - functie
    - gegevens voor verwerking
    - software
    - **configuratie** van de systemen
    - **credentials, toegangscontrole**(rollen, identiteiten),...

Bloomberg Businessweek

22/11/2015

Vulnerabilities!!!

met mogelijks heel grote impact naar patient safety!

Risico - Analyse
Vulnerabilities – Threats - Impacts

- *Complex geheel → grote 'attack surface'*
- *Een aanvaller hoeft slechts één maal, één zwak punt te vinden in het gehele complexe systeem.*
- *De verantwoordelijke dient **voortdurend** **alle punten** binnen de **perimeter** van zijn domein te beveiligen.*
- *De aanvaller gebruikt de initiële opening om een "command en control" structuur uit te bouwen en wist zijn sporen uit. (cfr. Botnet).*
- *Niet enkel technisch→ human factor (phising,...)*
- *De verantwoordelijke dient alert te blijven:*
  - **'intrusion detection' (bvb analyse van logdata)**
  - **Patchen van (gekende) vulnerabilities binnen redelijke termijn**
  - **...**

nothing can be said to be certain, except death and taxes ... and ICT vulnerabilities. (~ Benjamin Franklin)

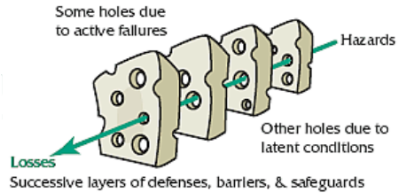
Sensibilisering !

"People don't react to reality;
they react to their perceptions of reality"

Sensibilisering is belangrijk !

juiste context !
geen "hypes" maar evenmin blindheid voor zorgwekkende evoluties/situaties !

The Swiss Cheese Model of Accident Causation



Achterhaald Paradigma : Domein & Perimeter

- *"Privacy" wetgeving bouwt op dit onderliggende centrale paradigma*
- *Mapping van wetsbegrippen naar ICT begrippen*
- *Immense uitdaging om die perimeter in stand te houden en te bewaken*
  - BYOD (Bring Your Own Device)
  - diverse "cloud" modellen en outsourcing
  - (potentiële) lekken via "toegangspunten"
    - proliferatie van "wireless" (BT, wifi, Zigbee, andere NFC,...)
    - "rogue" toegangspunten/overbruggingen...
  - hacking op complexe niveaus (incl. hardware/chipniveau), exploitatie van embedded systemen als entry point, rootkits,etc.
  - 0-day vulnerabilities, backdoors in legacy systems
  - **the "post-Snowden era" : exploitable backdoors in almost anything of importance !**

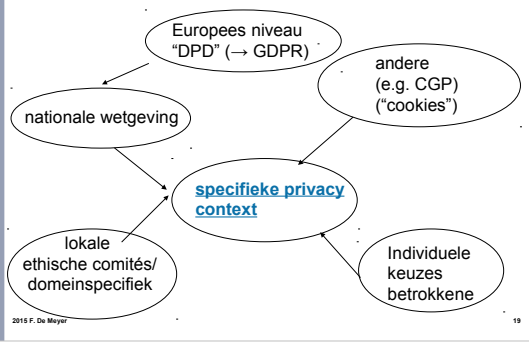
Verschillende invalshoeken m.b.t. '(Data in) Research'

- ***Wet Bescherming Persoonlijke Levenssfeer (WVP)--> PRIVACY***
  - **gebruik/communicatie van de gegevens**
  - **confidentialiteit en bescherming van de gegevens**
- *Ethical, Legal and Social Implications (ELSI) (incl. privacy)*
  - **naargelang type studie**
  - **ethische comités, GCP,**
- *Intellectual Property Rights (IPR)*
- *Research Ethics m.b.t. kwaliteit v.d. research (peer review, verifieerbaar, etc...)*
- *Commerciële partners of enkel/eveneens 'academische'*
  - **Voorschriften externe financiers (FWO, Horizon 2020)**
- *...*

Informaticagerelateerde misdrijven

- *delictomschrijving technologieneutraal → geen noodzaak specifieke wetgeving*
- *indien niet → nieuwe delictomschrijving invoeren*
- *technologie zowel middel als doel van criminaliteit*
- *wet inzake informaticacriminaliteit 28.11.2000 (BS 3.2.01)*
- *4 nieuwe misdrijven*
  - **valsheid in informatica**
  - **informaticabedrog**
  - **datamanipulatie**
  - **hacking**
- *invoering databeslag en netwerkzoeking*
- *aanpassing verplichtingen netwerkproviders / "derden"*

Complexiteit van privacy bescherming



WMA Helsinki declaration

- *(Ethical Principles for Medical Research Involving Human Subjects)*
- *Principle 20: " The subjects must be volunteers and informed participants in the research project."*
- *Principle 21: "Every precaution should be taken to respect the privacy of the subject,the confidentiality of the patient's information and to minimize the impact of the study on the subject's physical and mental integrity and on the personality of the subject."*

Various clinical trial references

- *ICH-GCP, FDA 21CFR part 11, part 312,...*

⇩

PRIVACY, PRIVACY, PRIVACY, PRIVACY, PRIVACY, PRIVACY, PRIVACY, PRIVACY, PRIVACY, PRIVACY, PRIVACY, PRIVACY, PRIVACY, PRIVACY, PRIVACY!

Note: informed consent is **not** a waiver for adequate privacy protection !

(consent is a legal basis for collecting and processing !)

Belgian legislation

- *Data protection law: 8.12.92/11.12.98*
- *Executive Royal Decree (KB): 13.2.2001*
- *Medical secrecy in penal code,...*
- *3 classes of data*
  - **Coded personal data**
  - **Non-coded personal data**
  - **Anonymous data**

Belgian Legislation (continued)

- *Primary vs. Secondary gathering*
- *Data processing by third party requires written contract with controller of data!*
- *Hierarchy of preferences*
  - **De-identified data**
  - **Coded (personal) data**
  - **Non-coded personal data (=identifiable)**
- *A processor that adds new data becomes controller !*
- *Reporting by controller to Data Protection Agency*

Privé-leven: Grondwettelijk Recht

- *GW Art.22 : "Ieder heeft recht op eerbiediging van zijn privé-leven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald."*
- *Uitzonderingen op het recht op eerbiediging van het privéleven kunnen enkel gemaakt worden door de wet.*
- *Een delegatie aan een andere macht is niet in strijd met het wettigheidsbeginsel voor zover de machtiging voldoende nauwkeurig is omschreven en betrekking heeft op de tenuitvoerlegging van maatregelen waarvan de essentiële elementen voorafgaandelijk door de wetgever zijn vastgelegd (advies Raad van State, nr. 45 540/1/2/3/4 van 15 en 17 december 2008).*

"Volgorde / Stappenplan"

- *Wetenschappelijke waarde en zin van een studie*
- *Haalbaarheid van de studie (resources, deelnemers, etc...)*
- *"ELSI":Ethical – Legal – Social Implications ?? → Ethisch comité (IRB, etc.)*
- *Oplossen van Privacy / Data Protectieproblemen*
  - Bij voorkeur ingebed in "ecosysteem" dat reeds cybersecurity garanties biedt
  - Waarvan de procedures, codes of conduct, etc gekend zijn en onderschreven door onderzoeker
  - Dient verder te gaan dan formalistische compliance
  - Vooral Data-Lifecycle denken !!

Samenvatting Privacyproblematiek (vanuit privacywetgeving)

- *Welke gegevens zullen worden verwerkt (proportionaliteit, finaliteit) ?*
- *Wie bepaalt de verwerking ?*
- *Wat is de wettelijke basis waarop de gegevens mogen worden verwerkt ?*
- *(aangiftes, machtiging, consent,etc..)*
- *Welke beschermingsmaatregelen van de gegevens worden genomen ?*
  - **m.b.t. identificeerbaarheid**
  - **m.b.t technische en organisatorische maatregelen om gegevenstoegang en -overdracht veilig uit te voeren**
- *Wat is de procedure ingeval er toch lekken optreden ?*
- *Life-cycle van de data (end-of-life van personal data) ?*

⇒ 'DATAMANAGEMENTPLAN'

Basisbeginselen Data-Collectie

- *Rechtmatigheids- en Doelgebondenheidsbeginsel*
  - de verwerking gebeurt "eerlijk".
  - voor een duidelijk aangekondigd doel.
  - niet langer bewaard dan noodzakelijk voor het doel.
  - nauwkeurig en juist !
- *Proportionaliteitsbeginsel*
  - de gegevensverzameling (aard, detail, hoeveelheid,...) is passend voor het doel.
  - de gegevens worden niet langer dan nodig bewaard (als persoonsgegeven).
- *Transparantiebeginsel ("informatieplicht")*
  - "data-subjecten" inlichten over doel en wie data inzamelt.
  - Info ivm het uitoefenen van inzagerecht
  - (aangifte bij CBPL)
- ***Wetenschappelijk onderzoek geniet van speciaal regime!***

De Verantwoordelijke voor de Verwerking

- *Bepaalt de doeleinden en de middelen.*
- *Bepaalt op welke manier de gegevens worden ingezameld.*
- *Bepaalt wie toegang mag hebben.*
- *Bepaalt wie ze mag verwerken of wijzigen.*
- *En onder welke voorwaarden dit kan gebeuren.*
- *Hij zorgt er ook voor dat er bewijzen zijn (wie?welke data?).*
- *(DPD--> "controller")*

Delegatie van taken ontslaat hem niet van zijn verantwoordelijkheid

Verwerking gevoelige gegevens ↔

(ras, gezondheid, politieke opvattingen, levensbeschouwelijke opvattingen)

- *uitdrukkelijke toestemming van de betrokken persoon;*
- *noodzakelijk om de betrokken persoon de nodige zorgen te verstrekken;*
- *verplicht door de arbeidswetgeving of met het oog op de toepassing van de sociale zekerheid;*
- *als de betrokkene de gegevens zelf openbaar heeft gemaakt;*
- *noodzakelijk voor de vaststelling, de uitoefening of de verdediging van een recht in rechte;*
- *noodzakelijk voor wetenschappelijk onderzoek (aangifte of machtiging)*

Praktisch

- *niet identificeerbaar → geen persoonsgegevens*
- *vrijstelling van aangifteplicht (meestal opdrachten overheid of heel courante verwerkingen met niet gevoelige gegevens).*
  - **Loon-en personeelsadministratie (KB Art. 51,52)**
  - **Boekhouding (KB Art.53)**
  - **Klanten- en leveranciersbeheer (KB Art.55)**
  - **VZWs (Art. 56)**
  - **....**
- *aangifteplicht (website CBPL)*
- *machtiging (sectoraal commité)*

Universitair Ziekenhuis Gent

CBPL "referentiemaatregelen"(1)

- *Informatiebeveiligingsbeleid (geschreven document)*
  - **Analyse en ricicobeheer toelichten**
  - **Beheersmaatregelen die worden genomen**
  - **Planning**
  - **Verantwoordelijken**
  - **Beheersproces bij beveiligingsincidenten**
  - **Sensibiliseringsproces van de instelling**
  - **Actualiseren van het beveilingssysteem**
- *Beveilingsconsulent*
- *Organisatie menselijke aspecten beveiliging*

Universitair Ziekenhuis Gent

CBPL "referentiemaatregelen"(2)

- *Fysieke beveiliging*
- *Beveiliging van netwerken*
- *Logische beveiliging van de toegang*
- *Logging, opsporing en analyse van toegang*
- *Toezicht, nazicht en onderhoud*
- *Beheer van beveiligingsincidenten en continuïteit*
- *Naleving*
- *Documentatie*

Universitair Ziekenhuis Gent

Opgelet! "CBPL Richtsnoeren"

- *CBPL Aanbeveling nr 01/2013 van 21 januari 2013.*
- *Aanbeveling uit eigen beweging betreffende de na te leven veiligheidsmaatregelen ter voorkoming van gegevenslekken (CO-AR-2013-001).*
- *"Een halt toe te roepen aan onbedoelde en ongeoorloofde gegevenslekken, de zogenaamde data breaches, die zoals zij vaststelde doorgaans te wijten zijn aan een onvoldoende gegevensbeveiliging".*
- *Een onvoldoende uitgebouwde informaticastructuur ligt daarbij veelal aan de basis van het probleem en vormt in combinatie met een gebrek aan voldoende ingebouwde controlemiddelen (het vierogenprincipe) en de afwezigheid van een systeem dat tijdig fouten detecteert en rechtzet, de ideale voedingsbodem voor gegevenslekken. Vanuit een permanente bekommernis om dergelijke situaties te voorkomen, formuleert de Commissie dan ook onderstaande aanbevelingen.*
- *CBPL document: "Richtsnoeren met betrekking tot de informatiebeveiliging van persoonsgegevens" (Versie 1.0 – Juni 2012).*

Universitair Ziekenhuis Gent

Wat met Wetenschappelijk Onderzoek ?

- *Wetenschappelijk onderzoek wordt steeds beschouwd als compatibel met het oorspronkelijke doel van de gegevensverzameling (doelgebondenheidsprincipe)*
- *Proportionaliteitsprincipe blijft overeind ! (enkel relevante en noodzakelijke gegevens)*
- *Vaak wordt afwijking toegestaan m.b.t. informatieplicht betrokkene.*
- ***Hiërarchie: anoniem → gecodeerd → niet gecodeerd***
- ***Steeds adequate bescherming garanderen!***
- *Aangifte CBPL ← verantwoordelijke verwerking expliciteren*

Universitair Ziekenhuis Gent

Hiërarchie van Identificeerbaarheid

- *Onderzoek gebeurt bij voorkeur met ge-anonimiseerde data, (zeker wat betreft secundair gebruik).*
- *Indien zulks niet mogelijk is, gebruikt de onderzoeker "gecodeerde data", met aangepaste gegevensbeveiliging.*
- *Indien ook dat niet mogelijk is, kan, mits motivatie, niet gecodeerde data (i.e. Identificeerbare data) gebruikt worden, met aangepaste gegevensbeveiliging.*
- *Geïnformeerde toestemming vragen aan betrokkene, behalve indien niet "haalbaar" (wordt heel vaak ingeroepen!).*

Universitair Ziekenhuis Gent

Terminologie !

Primaire verzameling/verwerking van gegevens

Onderzoek dat gebruik maakt van data die rechtstreeks bekomen zijn van betrokkenen die deelnemen aan het onderzoek

Secundaire verzameling/verwerking van gegevens

(i.e. "latere verwerking")

Onderzoek dat gebruik maakt van gegevens van betrokkenen die ooit verzameld zijn voor diagnostische- of zorgtoepassingen

Onderzoek dat gebruik maakt van gegevens van betrokkenen die in een ander onderzoek zijn verzameld, verwerkt.

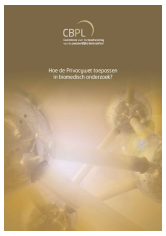
Universitair Ziekenhuis Gent

Biomedisch Onderzoek en de CBPL

http://www.privacycommission.be/nl

Universitair Ziekenhuis Gent

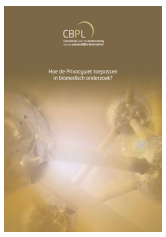
Voor het onderzoek start



- *Onderzoeksprotocol uitwerken*
- *Plan gegevensverzameling*
- *Beveiligingplan persoonsgegevens*
  - Identificatie / demografische data
  - "eigenlijke" onderzoeksdata
- *Data-subjecten ("betrokkenen") informeren*
- *En toestemming vragen (tenzij...)*
  - Opt in – opt out
- *Lijst personen gegevensverwerking + grond vertrouwelijkheid.*
- *Machtiging voor zorgsectorgegevens/Soc.Zek.*
- *Aangifte indienen (staat los v. machtiging)*

Universitair Ziekenhuis Gent

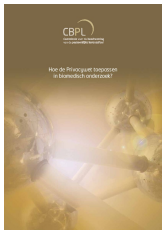
Tijdens onderzoek



- *Inzagerecht en recht op verbetering*
  - geen schade aan onderzoek toebrengen
  - desnoods uitstellen tot na onderzoek
  - Let wel: Wet Patiëntenrechten: strikter !
- *Opt-out door betrokkene*
  - kan op elk ogenblik
  - geen schadevergoeding (aan onderzoeker)
  - gegevens kunnen in onderzoek blijven
- *Beveiligen van gegevens !*
- *Minimalisatie van identificeerbaarheid*
  - anonimiseren
  - coderen (pseudoniemen)
  - bvb leeftijdscategorie ipv geboortedatum

Universitair Ziekenhuis Gent

Na het onderzoek



- *Publicatie gebeurt steeds anoniem !*
- *Indien niet meer nodig: vernietigen*
  - verwijderen 'persoonsgegeven'-eigenschap
  - opletten met re-identificatie !
- *Bewaren van data voor*
  - peer-reviews/verificatie
    - data
    - betrokkenen
  - biomedisch opvolginsonderzoek
- *Archiveren van Data*
  - aparte taak
  - beveiliging van archief
  - scheiden onderzoeksdata en ID-info
  - (metadata en kwaliteitsaspecten !)

Universitair Ziekenhuis Gent

Consent : 'Ge-informeerde Toestemming '

- *Sjablonen ontwikkeld (Nov 2011) door verschillende Belgische ethische comités, goedgekeurd door clinical trial taskforce op 26.06.2013*
- *4 verschillende sjablonen*
  - **basismodel interventionele studies volwassenen**
  - **extensie ivm wettelijke vertegenwoordiger**
  - **extensie ivm deelname in noodsituatie**
  - **basismodel niet interventionele studies (volwassenen)**

http://www.fagg-afmps.be/
nl/MENSELIJK_gebruik/geneesmiddelen/geneesmiddelen/onderzoek_ontwikkeling/ethisch_comite/sjablonen_geinformeerde_toestemming/

Universitair Ziekenhuis Gent

Wat (voorlopig nog) te doen (zorggegevens) ? (invoering GDPR kan procedure wijzigen)

- *Aanvragen machtiging bij Sectoraal Comité indien zulks van toepassing (gebruik RRN, communicatie overheids/KSZ databanken) en indien niet reeds gebeurd binnen de specifieke context)*
- *Aangifte CBPL (ongeacht machtiging)*
  - **(Gewone aangifte)**
  - **Aangifte van codering**
  - **Aangifte van latere werking van gecodeerde persoonsgegevens**
  - **Aangifte van latere verwerking van niet gecodeerde persoonsgegevens**

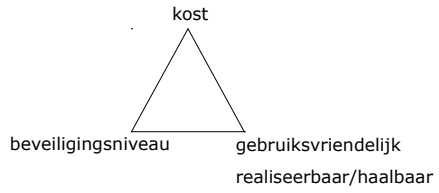
Brochure CBPL: Hoe de Privacywet toepassen in biomedisch onderzoek ?

Praktische tips cybersecurity

- *Voorschriften volgen m.b.t. gebruik van de systemen en toepassingssoftware (virus scanner,updates/patches...)*
- *Paswoordhygiëne*
  - Kies een relatief lang paswoord met hoofdletters, cijfers, (speciaal teken).
    Vb: Bevgep4OkcyWed3 (Bev-gep-FOUR-Ok-cy-Wed-THREE)
  - Dat niet in een woordenboek staat en niet via 'social engineering' af te leiden valt.
  - Kies verschillende paswoorden naargelang het systeem waarop je aanlogt.
  - Gebruik paswoordmanagersoftware en bewaar je veiligheidscopie op een veilige plaats.
  - Houdt paswoorden strikt geheim en deel ze met niemand.
- *Sla gevoelige data enkel op een beveiligde plaats op (betrouwbaar netwerk)*
- *Cave!! "Data on the move": USB sticks, externe harde schijven.*
  - Versleutel steeds! .
  - Wees voorzichtig met defecte of oude harde schijven, usb sticks, etc...
- *Beveilig/Bescherm steeds draagbare systemen (tablets, notebooks,etc..) en limiteer automatische login, zet sharing af!*
- *Cave!: inloggen via web-interface op "untrusted" platform (bvb in horeca)*
- *Cave!: publieke wifi toegang ! → gebruik een VPN toegang alvorens in te loggen op sites met gevoelige data en/of credentials.*
- *….*

Informatiebeveiliging-evenwichtsoefening

- technische haalbaarheid t.o.v. kost
- beveiligingsniveau en gebruiksvriendelijkheid



Diverse "Security Enhancing" Tools/Services

- *Sterk afhankelijk van type (platform): Windows, Mac, Linux*
- *File-encryption vs. Disk/partition encryption*
- *Keepass paswoord manager*
- *Truecrypt niet meer ondersteund! ⟶ Bitlocker*
- *Compressieprogramma met encryptie (vb: 7-zip)*
- *BoxCryptor : geschikt voor cloud toepassingen, usb sticks, etc...*
- *Disk Encryption nog voor het "booten"*
- *Sommige systemen laten "noodprocedure" toe om paswoord te resetten!*
- *Vertrouwelijke maildiensten: vb: tutanota.de*
- *Grondig en veilig wissen van oude media die gevoelige data bevat hebben.*
- *Defecte schrijven fysiek (laten) vernietigen of grondig wissen*
- *https://ssl-tools.net/*

- *Sterk afhankelijk van de kennis en ervaring van de gebruiker en versie van het gebruikersplatform !*

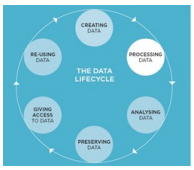
Datamanagement-Ugent: contactpunten

https://www.ugent.be/intranet/nl/op-het-werk/onderzoek-onderwijs/onderzoek/beleid/datamanagement

- *Infrastructuur voor databewaring, dataveiligheid en privacygevoelige data:* ***DICT***
- *Bewaren datasets gelinkt aan een publicatie in de academische bibliografie:* ***Biblio Helpdesk***
- *Octrooieerbare data en data voor derden:* ***Techtransfer***
  - **gebruik/communicatie van de gegevens**
  - **confidentialiteit en bescherming van de gegevens**

- *Opstellen van een Datamanagementplan*

Datamanagementplan (DMP)



- *~ ' Lifecycle denken '*
- *documenteren*
- *privacybepalingen*
- *contextuele vereisten (data, tools,...)*
  - FWO, HORIZON 2020
  - UK Research Councils: dmponline
- *Gecertificeerde repositories: Refs ?*
- *Registry of Research Data Repositories : http://service.re3data.org*
- *Dataopslag via Academische Bibliografie*
- *Om volledige integriteit te bewaren ('locking') zou een 'fingerprint' van de dataset moeten genomen worden en veilig bewaard ('forensische technieken')*
- *Wat met aspecten betreffende (re)identificatie ?*

UGENT: DICT

- *Centrale schijfruimte beheerd door DICT*
- *Backup en integriteit*
- *Onderscheid tussen (eigen) data opslaan en data delen ('share')*
- *Persoonlijke schijfruimte (gaat verloren als gebruiker Ugent verlaat)*
- *Binnen UZ/Ugent : privaat netwerwerk*
- *Van buiten UZ/Ugent: VPN : Virtual Private Netwerk*
- *Gebruiker: intern of extern aan UGENT ?*
- *Online shares zijn mogelijk.*
- *Gebruik externe cloud diensten enkel met (extra) encryptie.*

*https://www.ugent.be/**intranet**/nl/op-het-werk/onderzoek-onderwijs/onderzoek/beleid/kwaliteit/datamanagement*

Samenvatting Privacyproblematiek

- *Welke gegevens worden verwerkt (proportionaliteit, finaliteit) ?*
- *Door wie ?*
- *Wat is de wettelijke basis waarop de gegevens mogen worden verwerkt ?*
- *(aangiftes, machtiging, **consent**,etc..)*
- *Welke beschermingsmaatregelen van de gegevens worden genomen ?*
  - **m.b.t. identificeerbaarheid**
  - **m.b.t technische en organisatorische maatregelen om gegevenstoegang en -overdracht veilig uit te voeren**
- *Wat is de procedure ingeval er toch lekken optreden ?*
- *Life-cycle van de data (end-of-life van personal data) ?*

The future is …. GDPR……

- *15.12.2015 agreement*
- *4.5.2016 published in EU official Journal (after adoption)*
- *It shall apply from **25 May 2018***

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data,

and **repealing** Directive 95/46/EC (General Data Protection Regulation)

The (unresolved/introduced) issues too...

GDPR principes

- *Basis gelijkaardig aan DPD (Data Protection Directive)*
- *Accentverschuiving compliance → verantwoordelijkheid nemen voor effectieve risico-analyse en beveiliging*
- *Anonymous & Personal Data.*
- *"Data minimisation". Pseudonymised data is personal data !*
- *Art. 35 : Data Protection Impact Assessment ! ('PIA') = risk analysis*
- *Zeker indien "large scale" en "high risk" data.*
- *Art. 37-39 : Data Protection Officers (DPO) !*
- *Breach notification procedures (DPA & Data Subjects)*
- *The right to be forgotten*
- *Portability*
- *Records of Processing Activities*
- *Relatie tussen (joint) controller(s) en processors(s)*
- *Explicietere verantwoordelijkheid van processors.*
- *Codes of Conduct & Certification*
- *Binding Corporate Rules (Art. 47)*
- *Internationale Transfer van data / Expanded Territorial Scope*
- *Supervisory Authority ("DPA") & European Data Protection Board*
- *Boetes ("fines") !!!!!!!!!!!!!!!!*
- *Nog heel veel ruimte voor invulling door lidstaten (i.e. ambiguïteit) : chapt IX*

GDPR principes(vervolg)

- *Data Protection Impact Assessment uitvoeren als basis.*
- *om de nodige tegenmaatregelen te nemen.*
- *Data Protection by Design and by default (art.25)*
- *Transparantie in verwerkingsketen !! (controllers, processors)*
- *Overeenkomsten tussen controllers en processors*
- *(i.e. verantwoordelijken voor de verwerking en verwerkers)*
- *Enkel identificatie waar en zolang nodig !*
- *Data-minimisation & pseudonymisatie werken beschermend*
- *(maar het blijft personal data!!!)*

- *Er blijven echter heel onduidelijkheden en vragen !*
- *De gehoopte uniforme aanpak binnen de EU kan potentieel teniet gedaan worden door de keuzes die lidstaten kunnen maken, één van de huidige problemen !*
- *Risico op "shopping" naar landen met "least resistance" ?*

Thanks for listening !