Éthique et données : protection de la vie privée dès la conception (*privacy by design*)

Karën Fort

karen.fort@loria.fr / https://members.loria.fr/KFort

14 mars 2023

LETTRES SORBONNE UNIVERSITÉ

Loria Laboratoire lorrain de recherche en informatique et ses applications

PANTHÉON-ASSAS UNIVERSITÉ PARIS

Sources d'inspiration

- edX MOOC de l'Université du Michigan (2016) : *Data Science Ethics*
- *Ethical IT Innovation* (2016). S. Spiekermann. CRC Press.
- *Privacy by Design: the 7 Foundational Principles* (2011). Ann Cavoukian.
- *OWASP Top 10 Privacy Risks Project*
- *Engineering Privacy by Design* (2017). Carmela Troncoso.
- Wikipedia

Principes de la protection de la vie privée dès la conception
Les 7 principes fondateurs
Vue du RGPD

Mettre en œuvre la protection de la vie privée dès la conception

Pour finir

Principes de la protection de la vie privée dès la conception
Les 7 principes fondateurs
Vue du RGPD

Mettre en œuvre la protection de la vie privée dès la conception

Pour finir

1. Prendre des mesures proactives et non réactives, préventives et non correctives

- prévoir et prévenir les problèmes **avant** qu'ils se produisent
- n'offre aucune solution pour résoudre les problèmes une fois qu'ils apparaissent

2. Assurer une protection "par défaut" de la vie privée

Aucune action n'est nécessaire de la part de l'individu pour protéger sa vie privée

le système est conçu comme protecteur, **par défaut**

3. Intégrer la protection de la vie privée dans la conception des systèmes

La protection de la vie privée n'est pas une option

c'est un **composant essentiel** de la fonctionnalité de base du système

4. Assurer la protection de la vie privée sans nuire à la mise en œuvre d'autres fonctionnalités

satisfaire tous les intérêts et objectifs légitimes

Pas de compromis inutile

5. Assurer la sécurité de bout en bout

La protection de la vie privée doit être assurée pendant tout le cycle de vie des données impliquées

toutes les données doivent être **conservées de manière sécurisée**, puis **détruites de manière sécurisée** à la fin des traitements

6. Assurer la visibilité et la transparence

à faire vérifier de manière indépendante

Les composants comme les opérations doivent rester **visibles** et **transparents** aux utilisateurs et aux fournisseurs

7. Respecter la vie privée des utilisateurs

Privilégier les intérêts des individus :

- fonctionnalités par défaut de protection de la vie privée
- information appropriée
- options faciles à utiliser

Principes de la protection de la vie privée dès la conception
Les 7 principes fondateurs
Vue du RGPD

Mettre en œuvre la protection de la vie privée dès la conception

Pour finir

Le RGPD : https://xkcd.com/1998/

PRIVACY POLICY

WE'VE UPDATED OUR PRIVACY POLICY. THIS IS PURELY OUT OF THE GOODNESS OF OUR HEARTS, AND HAS NOTHING TO DO WITH ANY HYPOTHETICAL UNIONS ON ANY PARTICULAR CONTINENTS. PLEASE READ EVERY PART OF THIS POLICY CAREFULLY, AND DON'T JUST SKIP AHEAD LOOKING FOR SEX SCENES.

THIS POLICY GOVERNS YOUR INTERACTIONS WITH THIS WEBSITE, HEREIN REFERRED TO AS "THE SERVICE," "THE WEBSITE," "THE INTERNET," OR "FACEBOOK," AND WITH ALL OTHER WEBSITES AND ORGANIZATIONS OF ANY KIND. THE ENUMERATION IN THIS POLICY, OF CERTAIN RIGHTS, SHALL NOT BE CONSTRUED TO DENY OR DISPARAGE OTHERS RETAINED BY THE USERS. BY USING THIS SERVICE, YOU OPT IN TO QUARTERING TROOPS IN YOUR HOME.

YOUR PERSONAL INFORMATION

PLEASE DON'T SEND US YOUR PERSONAL INFORMATION. WE DO NOT WANT YOUR PERSONAL INFORMATION. WE HAVE A HARD ENOUGH TIME KEEPING TRACK OF OUR *OWN* PERSONAL INFORMATION, LET ALONE YOURS.

IF YOU TELL US YOUR NAME, OR ANY IDENTIFYING INFORMATION, WE WILL FORGET IT IMMEDIATELY. THE NEXT TIME WE SEE YOU, WE'LL STRUGGLE TO REMEMBER WHO YOU ARE, AND TRY DESPERATELY TO GET THROUGH THE CONVERSATION SO WE CAN GO ONLINE AND HOPEFULLY FIGURE IT OUT.

TRACKING PIXELS, COOKIES, AND BEACONS

THIS WEBSITE PLACES PIXELS ON YOUR SCREEN IN ORDER TO FORM TEXT AND IMAGES, SOME OF WHICH MAY REMAIN IN YOUR MEMORY AFTER YOU CLOSE THE PAGE. WE USE COOKIES TO ENHANCE YOUR PERFORMANCE. OUR WEBSITE MAY USE LOCAL STORAGE ON YOUR DEVICE IF WE RUN LOW ON SPACE ON OUR END. WE MAY USE BEACONS TO CALL ROHAN FOR AID.

3RD PARTY EXTENSIONS

THIS SERVICE MAY UTILIZE 3RD PARTY EXTENSIONS IN ORDER TO PLAY THE SONG ***CAN U FEEL IT*** FROM THEIR DEBUT ALBUM ***ALIVE.***

PERMISSION

FOR USERS WHO ARE CITIZENS OF THE EUROPEAN UNION, WE WILL NOW BE REQUESTING PERMISSION BEFORE INITIATING ORGAN HARVESTING.

SCOPE AND LIMITATIONS

THIS POLICY SUPERSEDES ANY APPLICABLE FEDERAL, STATE, AND LOCAL LAWS, REGULATIONS AND ORDINANCES, INTERNATIONAL TREATIES, AND LEGAL AGREEMENTS THAT WOULD OTHERWISE APPLY. IF ANY PROVISION OF THIS POLICY IS FOUND BY A COURT TO BE UNENFORCEABLE, IT NEVERTHELESS REMAINS IN FORCE.

THIS ORGANIZATION IS NOT LIABLE AND THIS AGREEMENT SHALL NOT BE CONSTRUED. THESE STATEMENTS HAVE NOT BEEN EVALUATED BY THE FDA. THIS WEBSITE IS INTENDED TO TREAT, CURE, AND PREVENT ANY DISEASE.

IF YOU KNOW ANYONE IN EUROPE, PLEASE TELL THEM WE'RE COOL.

Article 25 - Protection des données dès la conception et protection des données par défaut

Article 25 - Protection des données dès la conception et protection des données par défaut

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.

2. Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.

3. Un mécanisme de certification approuvé en vertu de l'article 42 peut servir d'élément pour démontrer le respect des exigences énoncées aux paragraphes 1 et 2 du présent article.

https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4


LE RESPONSABLE
DU TRAITEMENT DOIT...
COMMENT ??
imgflip.com

Principes de la protection de la vie privée dès la conception

Mettre en œuvre la protection de la vie privée dès la conception

- Applications Web
- Minimisation
- Anonymisation vs pseudonymisation

Pour finir

Principes de la protection de la vie privée dès la conception

Mettre en œuvre la protection de la vie privée dès la conception
- Applications Web
- Minimisation
- Anonymisation vs pseudonymisation

Pour finir

Top 10 des risques concernant la vie privée dans les applications Web (OWASP)

- P1 Web Application Vulnerabilities
- P2 Operator-sided Data Leakage
- P3 Insufficient Data Breach Response
- P4 Insufficient Deletion of personal data
- P5 Non-transparent Policies, Terms and Conditions
- P6 Collection of data not required for the primary purpose
- P7 Sharing of data with third party
- P8 Outdated personal data
- P9 Missing or Insufficient Session Expiration
- P10 Insecure Data Transfer

Détails :

https ://www.owasp.org/images/0/0a/OWASP_Top_10_Privacy_Countermeasures_v1.0.pdf

Grille OWASP : forces

How to check?	Countermeasures
General questions: • Is an incident response plan for privacy incidents in place?	Countermeasures (in advance): • Create and maintain incident response plan.

→ une grille d'analyse précise et pragmatique (directement applicable)

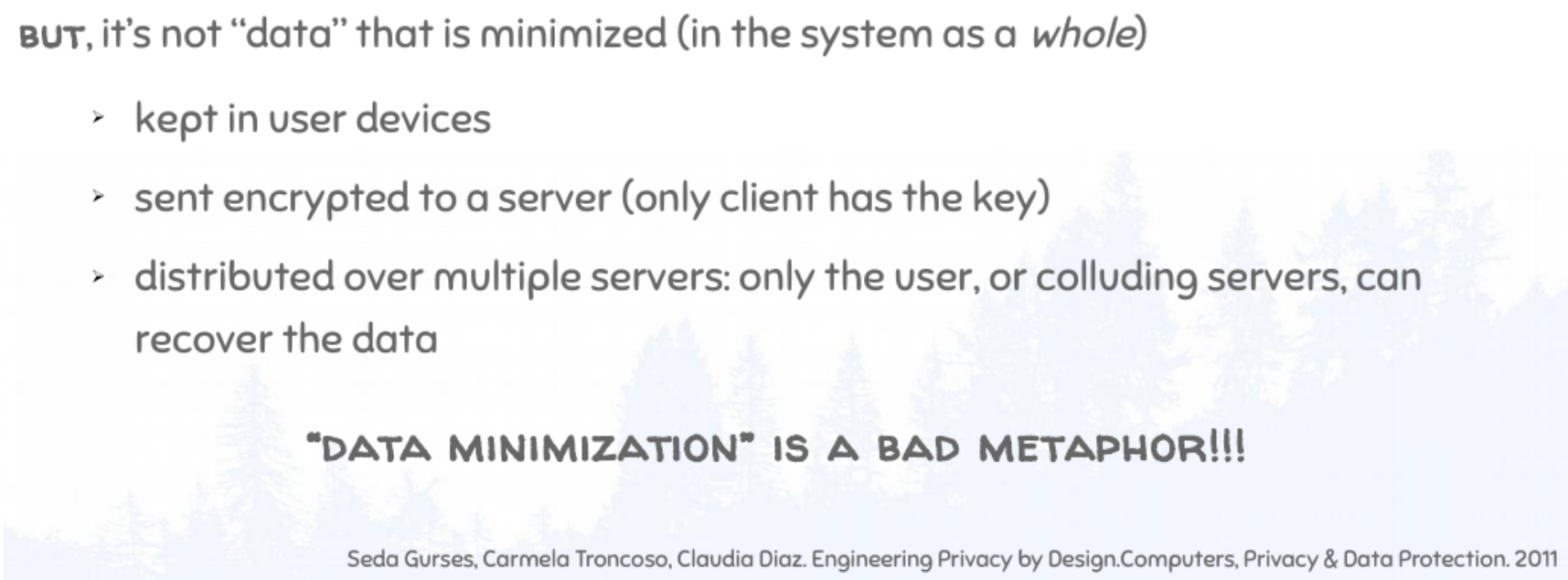
Principes de la protection de la vie privée dès la conception

Mettre en œuvre la protection de la vie privée dès la conception
- Applications Web
- Minimisation
- Anonymisation vs pseudonymisation

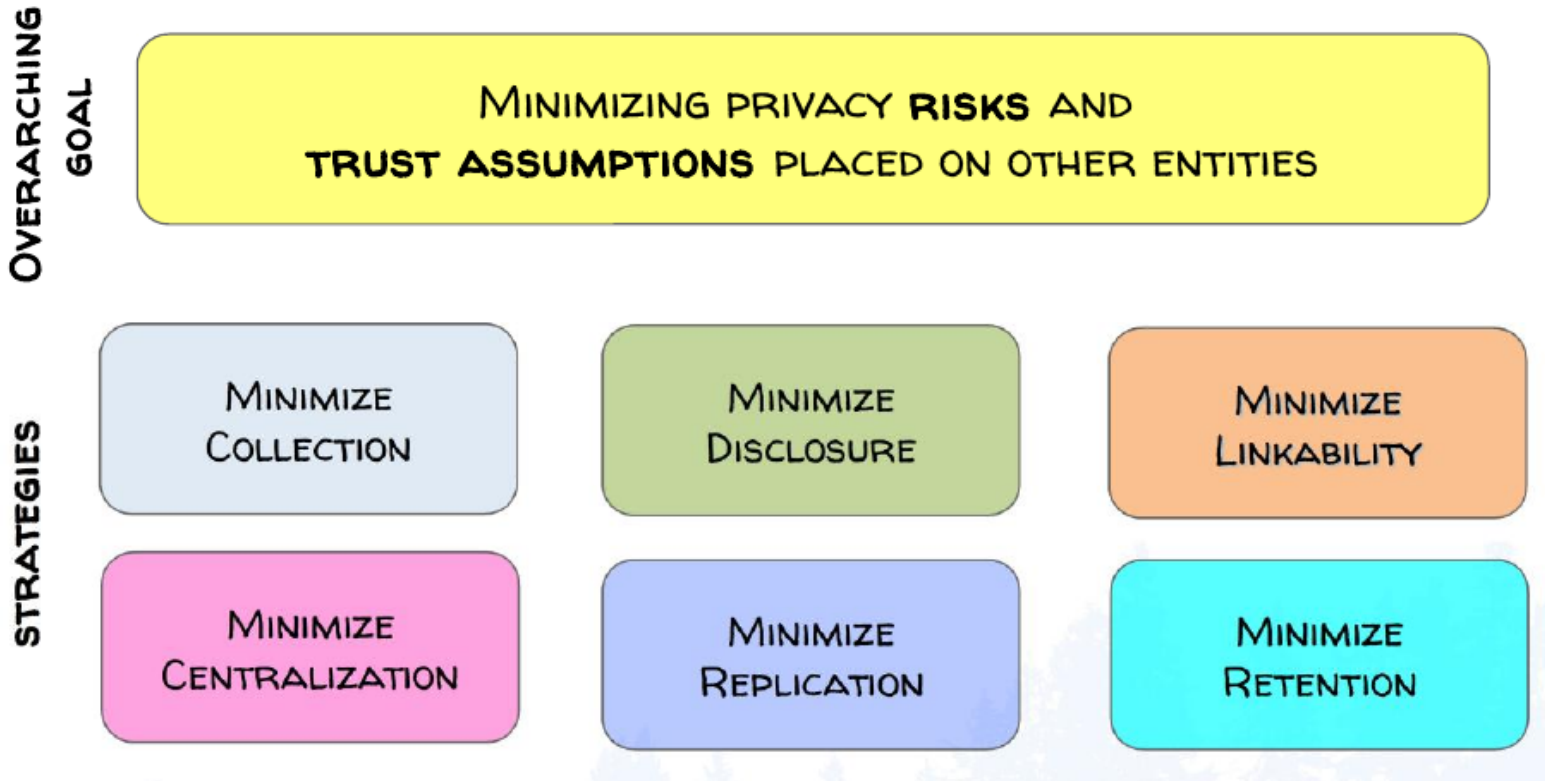
Pour finir

La protection de la vie privée comme exercice de contrôle

La minimisation des données est une "première étape nécessaire et fondamentale" [Gurses et al., 2011]

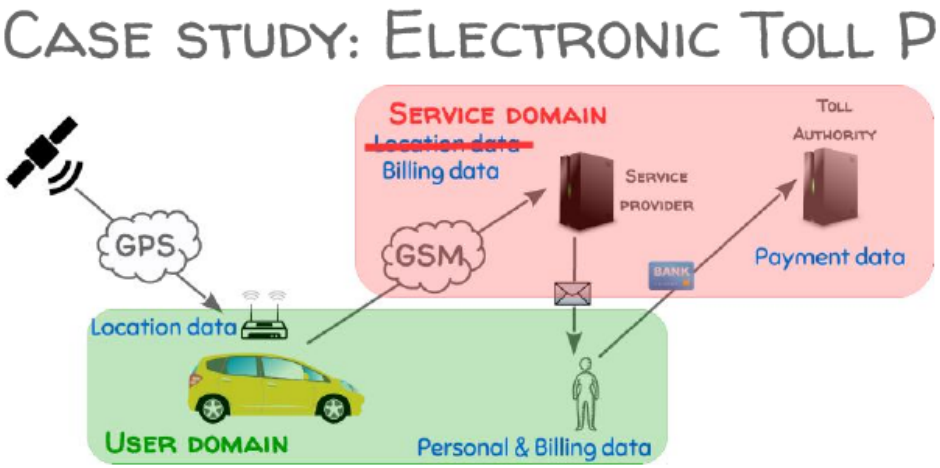


Stratégies de minimisation des données



[Gurses et al., 2011]

Exemple



Location is not needed,
only the amount to bill!

[Gurses et al., 2011]

Principes de la protection de la vie privée dès la conception

Mettre en œuvre la protection de la vie privée dès la conception
- Applications Web
- Minimisation
- Anonymisation vs pseudonymisation

Pour finir

Désidentification/pseudonymisation : efficacité ?

Le code postal, la date de naissance et le sexe ne sont pas considérées comme des données personnelles identifiantes

Cependant, 87 % des numéros de sécurité sociale US peuvent être retrouvés uniquement à partir de ces 3 informations... (edX MOOC)

La désidentification peut être facilement contournée en :

- récupérant des données identifiantes
- reliant des identifiants partiels multiples
- utilisant des jeux de données externes

Anonymisation : un processus irréversible

https://cer.sorbonne-universite.fr/ressources-ethiques

Le processus d'anonymisation vise à éliminer toute possibilité de ré-identification :

- il ne doit pas être possible d'isoler un individu dans le jeu de données
- il ne doit pas être possible de relier entre eux des ensembles de données distincts concernant un même individu
- il ne doit pas être possible de déduire, de façon quasi certaine, de nouvelles informations sur un individu

La phrase suivante nest pas anonyme (alors quelle ne contient aucun nom) :

Le fils du Premier Ministre de Fridonie est schizophrène.

Désidentification vs anonymisation : facilité ?

Facile :

Mme X... a eu connaissance de ce que l'arrêt de la cour d'appel de Douai avait été publié sur Internet sans être anonymisé

http://www.precisement.org/blog/

Defaut-d-anonymisation-d-un-arret-sur-Legifrance-l-Etat-condamne-a-1000-euros.html

Moins facile :

Le maire d'Agnos, président de la Fédération des œuvres laïques (FOL) de 1999 à 2003, a été condamné par la cour d'appel de Pau à 2 ans de prison avec sursis

https://www.visualiserlacorruption.fr/acts/47e07606

Principes de la protection de la vie privée dès la conception

Mettre en œuvre la protection de la vie privée dès la conception

Pour finir

CQFR : Ce Qu'il Faut Retenir

- Principes
- Minimisation
- Anonymisation vs pseudonymisation


Gurses, S., Troncoso, C., and Diaz, C. (2011).
Engineering privacy by design.
In Computers, Privacy & Data Protection.