

Pseudonymisation: Feedback from the CNIL

Monir Azraoui – CNIL

Technology expert

December 9th, 2021

About the CNIL: Missions

- ◊ Informs & Protects
- ◊ Supports & Guides
- ◊ Audits & Sanctions
- ◊ Anticipates & Encourages Innovation

- ◊ Team of +200 Law & Technology experts



Pseudonymisation in the GDPR

Pseudonymisation

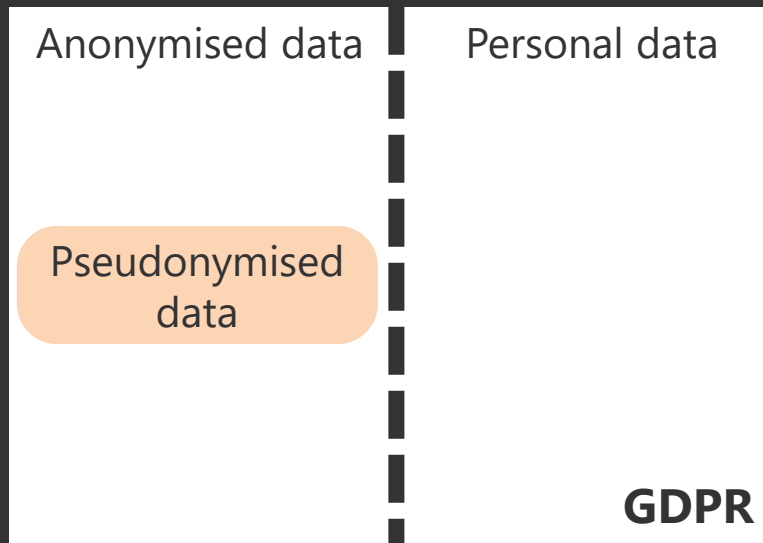
Recital (26):

Personal data which have undergone **pseudonymisation**, which could be attributed to a natural person by the use of **additional information** should be considered to **be information on an identifiable natural person**.

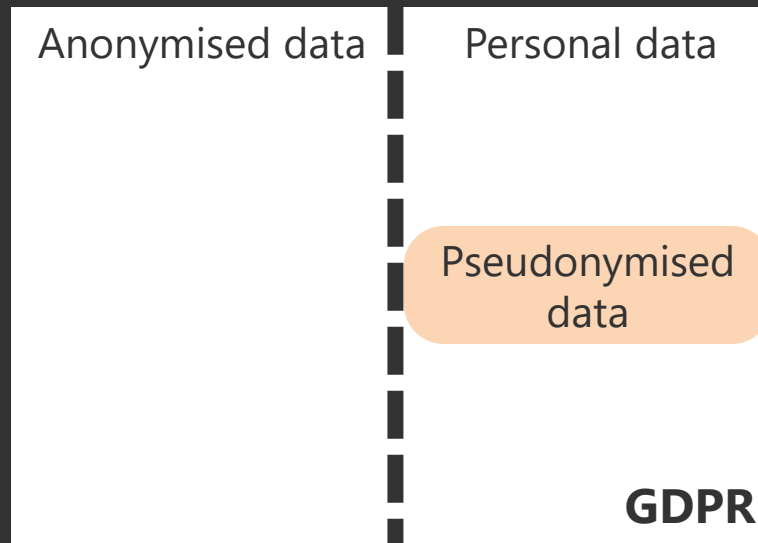
Article 4 (5):

'**pseudonymisation**' means the processing of personal data in such a manner that the personal data can **no longer be attributed to a specific data subject** without the use of **additional information**, provided that such additional information is **kept separately and is subject to technical and organisational measures** to ensure that the personal data are not attributed to an identified or identifiable natural person

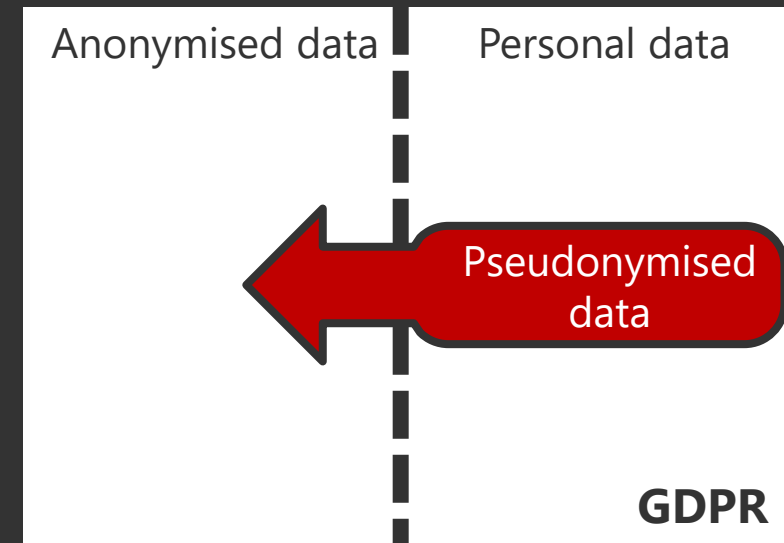
PSEUDONYMISATION VS. ANONYMISATION



HOW DATA CONTROLLERS SEE IT



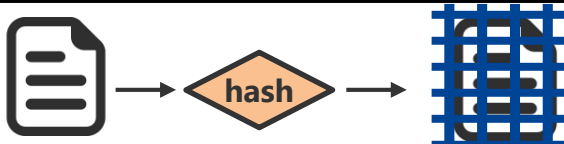
HOW THE GDPR SEES IT



WHAT DATA CONTROLLERS WANT

Audits reveal bad practices...

- Ex-post audits to check whether DCs comply with the law




Hashing as an anonymisation mechanism

name	job	city	car
XXX	lawyer	Cannes	Jaguar
YYY	doctor	Nice	Lexus

Removing direct identifiers as an anonymisation mechanism

Misunderstanding of pseudonymisation/anonymisation



Weak cryptographic keys

~~SHA-1~~
~~MD5~~

Obsolete hashing algorithms

Bad implementation of pseudonymisation mechanisms



No plan to refresh cryptographic keys



No technical measures to protect secrets/additional info



No organisational measures to ensure confidentiality of secrets/additional info


Inadequate measures to protect "additional information"

... and good practices!

- Ex-post audits to check whether DCs comply with the law




Re-identification risk analysis performed



Secure storage of cryptographic keys or secrets

Plan to refresh cryptographic keys

Protection of "additional information"



Encryption of pseudonymised files

name	job	city	car
XXX	lawyer	France	Jaguar
YYY	doctor	France	Lexus

k-anonymity
l-diversity

Combination of pseudonymisation with other security techniques

RELEVANT USE CASES

Use Case #1: partitioning data

Police records transcription

GENDARMERIE NATIONALE		ENQUÊTE PRÉLIMINAIRE	
Compagnie MORTAGNE AU PERCHE Communauté de brigades de L'AIGLE		PROCÈS-VERBAL DE DÉGRADATIONS	
Code Unité 01095	P.V. 02351	Année 2007	N° pièce 01
Salaire		Événement	Date 08/09/2007
Faits DÉGRADATION OU DETERIORATION GRAVE D'UN BIEN APPARTENANT A AUTRUI NATIF			
Références du 15/11/2005 à 08:00 au 08/09/2007 à 11:45 Code Postal, Commune 61270 RAI Adresse de commission du fait résidence secondaire site lieu de [REDACTED] 9833 Pénal ART.322-1 AL.1, C.PENAL. Niveau ART.322-1 AL.1, ART.322-15 1° 2° 3° 5° C.PENAL.			
Le samedi 8 septembre 2007 à 16 heures 30 minutes Nous soussigné Gendarme [REDACTED] Agent de Police Judiciaire en résidence à L'AIGLE Sous le contrôle de : Maréchal des Logis Chef [REDACTED], Officier de Police Judiciaire en résidence à L'AIGLE Vu les articles 20, 21-1 et 75 à 78 du Code de Procédure Pénale Nous trouvant au bureau de notre unité à L'AIGLE, rapportons les opérations suivantes :			
IDENTITÉ DE LA VICTIME			
Nom	Prénoms	Nom Marital	
[REDACTED]	[REDACTED]	[REDACTED]	
Sexe	Situation de Famille	Date Naissance	Code Postal et Commune Naissance
[REDACTED]	[REDACTED]	[REDACTED]	VITRY SUR SEINE (94) (France)
Adresse		N° de Tél.Équipe	Profession
[REDACTED]		[REDACTED]	[REDACTED]
Code Postal et Commune	Nationalité (si étranger)		
[REDACTED]	France		
Entendons la personne dénommée ci-dessus qui nous déclare en tant que 'PROPRIÉTAIRE			
DATE OU PERIODE ET LIEU DES FAITS			
Période du 15/11/2005 à 08 heures 00 au 08/09/2007 à 11 heures 45 minutes, dans une résidence secondaire site lieu de [REDACTED] à 61270 RAI			
CONSTATATIONS (inscriptions utiles, matériel trouvé)			
Les carreaux de 03 fenêtres extérieures et de 04 portes ont été cassés. Le ou les auteurs sont entrés par l'arrière de l'habitation en fracturant la porte donnant sur le garage. Il ont jeté leur dévolu exclusivement sur les pièces du rez de chaussée de la résidence secondaire. A l'intérieur de l'habitation, les mobiliers et des accessoires de la cuisine, du séjour, du garage et d'une cave ont été saccagés. De l'huile a été répandue sur le sol de différentes pièces. Des papiers peints ont été arrachés. Des prises électriques ont été arrachées. Des inscriptions ont été mises sur le papier peint du séjour et de la cuisine à l'aide d'une bombe de peinture de couleur noire. Dans le séjour, l'inscription " Nous on é de la madeleine é on en é fière !! métaphore." est visible. Dans la cuisine, deux logos du sigle de l'anarchie sont visibles. Un frigidaire a été renversé. Une tondeuse, une pelle, une pioche et deux jantes de véhicule ont été déplacées de la cave au séjour. Aucun objet n'a été volé. Les huisseries de deux portes ont été cassées. Dans la chambre du rez de chaussé, une armoire en bois a été renversée et cassée.			
MESURES PRISES			
Des prises de vue photographiques ont été réalisées.			
Vu et transmis par : [Signature]			
(DESTINATAIRES)			
[2] - M. le procureur de la République à ALENCON			
[1] - Archives à L'AIGLE			

GENDARMERIE NATIONALE		ENQUÊTE PRÉLIMINAIRE	
Compagnie MORTAGNE AU PERCHE Communauté de brigades de L'AIGLE		PROCÈS-VERBAL DE DÉGRADATIONS	
Code Unité 01095	P.V. 02351	Année 2007	N° pièce 01
Salaire		Événement	Date 08/09/2007
Faits DÉGRADATION OU DETERIORATION GRAVE D'UN BIEN APPARTENANT A AUTRUI NATIF			
Références du 15/11/2005 à 08:00 au 08/09/2007 à 11:45 Code Postal, Commune 61270 RAI Adresse de commission du fait résidence secondaire site lieu de [REDACTED] 9833 Pénal ART.322-1 AL.1, C.PENAL. Niveau ART.322-1 AL.1, ART.322-15 1° 2° 3° 5° C.PENAL.			



GENDARMERIE NATIONALE		ENQUÊTE PRÉLIMINAIRE	
Compagnie MORTAGNE AU PERCHE Communauté de brigades de L'AIGLE		PROCÈS-VERBAL DE DÉGRADATIONS	
Code Unité 01095	P.V. 02351	Année 2007	N° pièce 01
Salaire		Événement	Date 08/09/2007
Faits DÉGRADATION OU DETERIORATION GRAVE D'UN BIEN APPARTENANT A AUTRUI NATIF			
Références du 15/11/2005 à 08:00 au 08/09/2007 à 11:45 Code Postal, Commune 61270 RAI Adresse de commission du fait résidence secondaire site lieu de [REDACTED] 9833 Pénal ART.322-1 AL.1, C.PENAL. Niveau ART.322-1 AL.1, ART.322-15 1° 2° 3° 5° C.PENAL.			

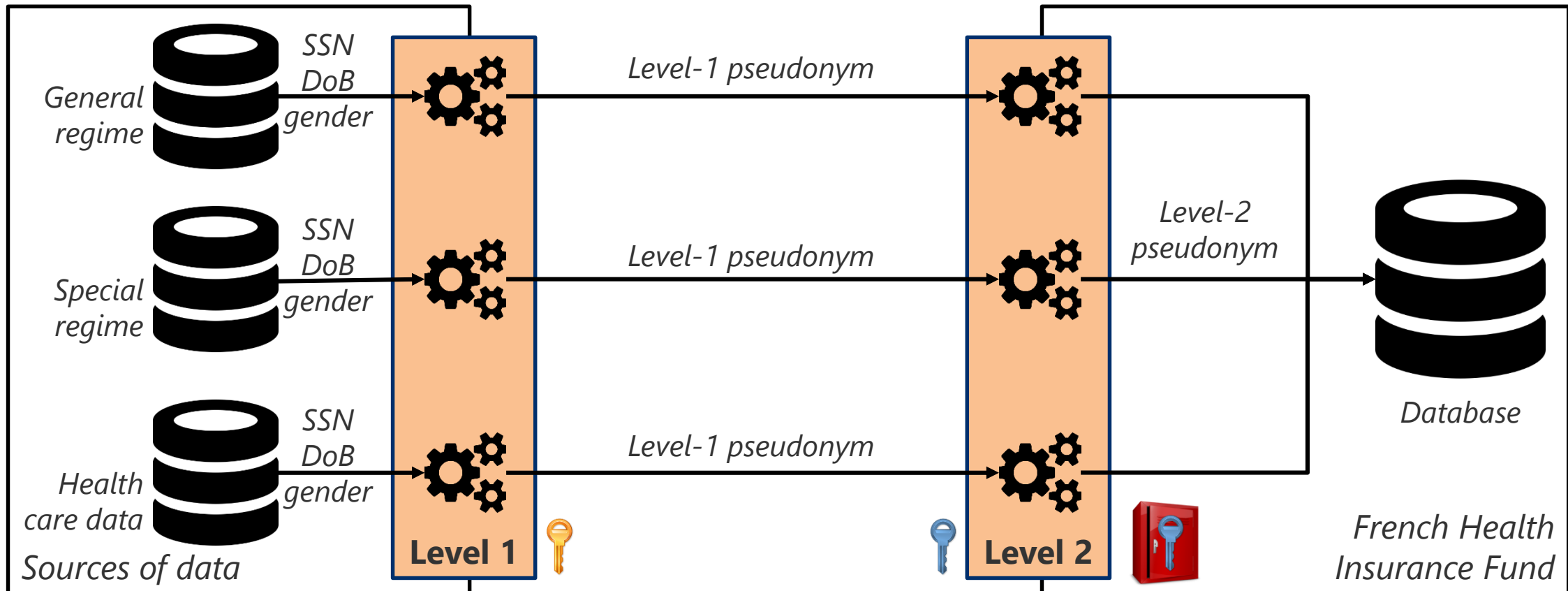


GENDARMERIE NATIONALE		ENQUÊTE PRÉLIMINAIRE	
Compagnie MORTAGNE AU PERCHE Communauté de brigades de L'AIGLE		PROCÈS-VERBAL DE DÉGRADATIONS	
Code Unité 01095	P.V. 02351	Année 2007	N° pièce 01
Salaire		Événement	Date 08/09/2007
Faits DÉGRADATION OU DETERIORATION GRAVE D'UN BIEN APPARTENANT A AUTRUI NATIF			
Références du 15/11/2005 à 08:00 au 08/09/2007 à 11:45 Code Postal, Commune 61270 RAI Adresse de commission du fait résidence secondaire site lieu de [REDACTED] 9833 Pénal ART.322-1 AL.1, C.PENAL. Niveau ART.322-1 AL.1, ART.322-15 1° 2° 3° 5° C.PENAL.			



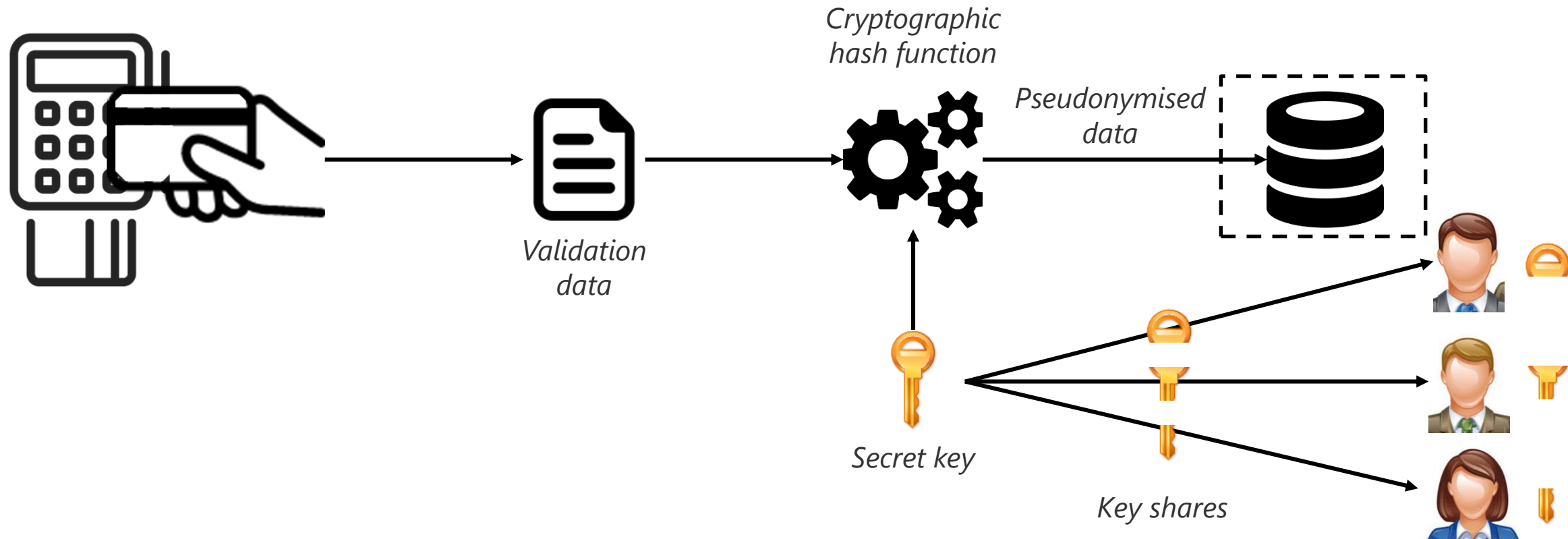
Use Case #2: 2-level pseudonymisation

- French Health Insurance Information System



Use case #3: hashing and key splitting

- Ticketing data in public transportation systems (fraud)



Main takeaways & Recommendations

- Pseudonymisation often mistaken with anonymisation by DC
 - Misunderstanding of the benefits of pseudonymisation by DC
- Practical pseudonymisation: a variety of techniques
 - Have your pseudonymisation procedure evaluated by experts
 - Implement tailored privacy & security measures to your processing
- Determine risks of re-identification
 - residual

CNIL.

THANK YOU