inventeurs du monde numérique

Échelle de sensibilité des données d'Inria

Échelle de sensibilité

1. Pourquoi une échelle de sensibilité ?
2. Méthodologie
3. Comment ça marche ?

1. Échelle de sensibilité

Pourquoi une échelle de sensibilité ?

À quoi ça sert ?

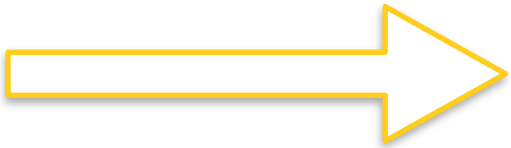
Se donner un vocabulaire commun

Alice

Bob

Confidentiel

Nam tempus feugiat elit, vel tristique dolor. Vivamus sagittis augue ac eros tempor porttitor. Nam tempus lorem non nisi tempor, in mollis sapien lobortis. Praesent blandit quam nec purus venenatis laoreet.



Confidentiel

Nam tempus feugiat elit, vel tristique dolor. Vivamus sagittis augue ac eros tempor porttitor. Nam tempus lorem non nisi tempor, in mollis sapien lobortis. Praesent blandit quam nec purus venenatis laoreet.

« C’est confidentiel, ne pas retransmettre, ça reste entre toi et moi »

« C’est confidentiel, à envoyer seulement à des personnes de confiance »

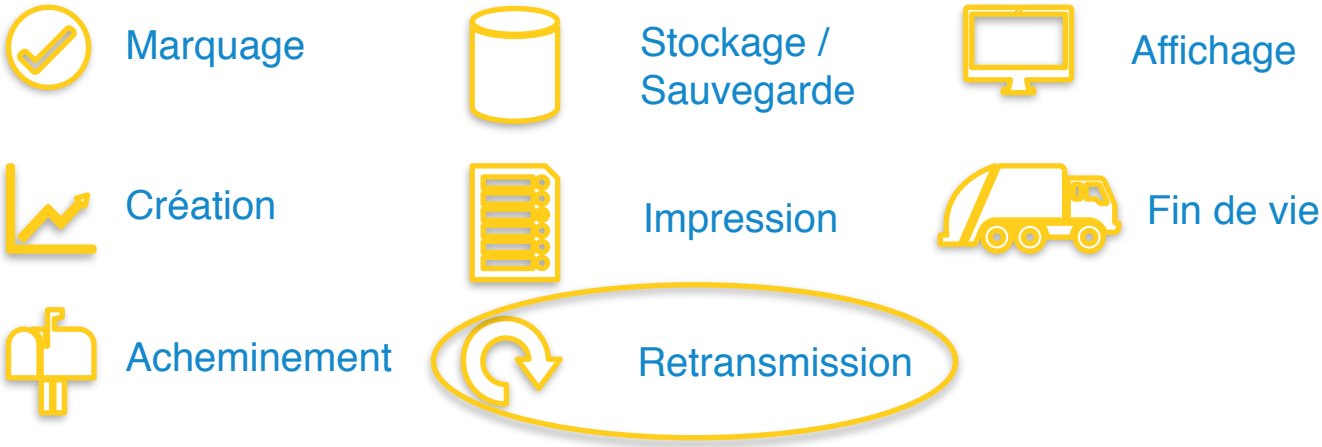
À quoi ça sert ?

Se donner un vocabulaire commun

À quoi ça sert ?

Se donner un vocabulaire commun

Décrire les actions associées à la classification d'une information



À quoi ça sert ?

Se donner un vocabulaire commun

Décrire les actions associées à la classification d'une information

Utiliser une solution d'échange numérique adéquate

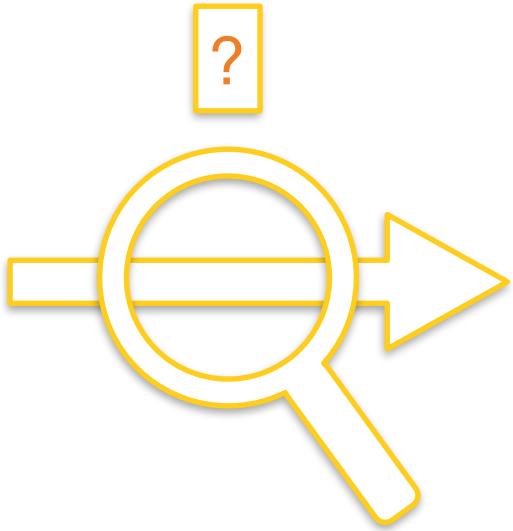
À quoi ça sert ?

Utiliser une solution d'échange numérique adéquate

Alice

Confidentiel

Nam tempus feugiat elit, vel tristique dolor. Vivamus sagittis augue ac eros tempor porttitor. Nam tempus lorem non nisi tempor, in mollis sapien lobortis. Praesent blandit quam nec purus venenatis laoreet.



Bob

Confidentiel

Nam tempus feugiat elit, vel tristique dolor. Vivamus sagittis augue ac eros tempor porttitor. Nam tempus lorem non nisi tempor, in mollis sapien lobortis. Praesent blandit quam nec purus venenatis laoreet.

Est-ce que c'est une obligation ?

PSSI de l'État => PSSI Inria

Instruction Interministérielle 901

Guide méthodologique sur la protection
des informations numériques sensibles liées aux
activités des ZRR

RGPD

Est-ce que c'est une obligation ?

PSSI de l'État => PSSI Inria

Instruction Interministérielle 901

Guide méthodologique sur la protection des informations numériques sensibles liées aux activités des ZRR

RGPD

2. Échelle de sensibilité

Méthodologie

Des règles internes

Politique Générale de Sécurité de l'information (2015)

Inria met en place une échelle de sensibilité des données, informe les collaborateurs de l'existence de cette échelle, définit des règles de fonctionnement pour les données les plus sensibles et propose des outils de protection adaptés.

Règlement Intérieur d'Inria (2017)

- Chaque collaborateur Inria doit évaluer le niveau de confidentialité des données professionnelles dont il est producteur et les protéger en utilisant les outils adaptés, en conformité avec les recommandations d'Inria.
- Lorsqu'un document est marqué avec un niveau de confidentialité issu de l'échelle de sensibilité en vigueur, le collaborateur Inria applique les règles d'utilisation adaptées à ce niveau de confidentialité.

Une classification partagée

Inria

Rédacteurs : FSD, RSSI, DPD

Relecture : ~80 personnes. CUMI, COERLE, COSS I&SSI, CSSI

CNRS

Rédacteurs : RSSI

Relecture : FSD, DAJ

INRA

Rédacteurs : FSD, RSSI

Relecture : Instances sécurité

Document diffusé aux RSSI du MESRI.

Mise en œuvre prévue/ évoquée :
Université de Lorraine
Université de Rennes 1
…

3. Échelle de sensibilité

Comment ça marche ?

Détermination de la sensibilité

Comment mesure-t-on la sensibilité d'une information ?

On mesure la sensibilité en fonction de l'impact potentiel en cas de diffusion hors du périmètre prévu

Quels sont les différents impacts possibles ?

- Conséquences juridiques
- Image
- Conséquences financières
- PPST
- Conséquences sur les personnes
- Conséquences pour la Nation

Exemple : RGPD

Impact
Nul
Modéré
Important
Catastrophique

Exemple : RGPD

Niveau de classification	Impact
Public	Nul
Diffusion Limitée	Modéré
Confidentiel	Important
Diffusion Restreinte (II 901)	Catastrophique

Exemple : RGPD

Niveau de classification	Impact	Conséquences sur les personnes (RGPD, CNIL)
Public	Nul	
Diffusion Limitée	Modéré	
Confidentiel	Important	
Diffusion Restreinte (II 901)	Catastrophique	

Exemple : RGPD

Niveau de classification	Impact	Conséquences sur les personnes (RGPD, CNIL)
Public	Nul	
Diffusion Limitée	Modéré	
Confidentiel	Important	
Diffusion Restreinte (II 901)	Catastrophique	

Exemple : RGPD

Niveau de classification	Impact	Conséquences sur les personnes (RGPD, CNIL)
Public	Nul	Aucune
Diffusion Limitée	Modéré	
Confidentiel	Important	
Diffusion Restreinte (II 901)	Catastrophique	

Exemple : RGPD

Niveau de classification	Impact	Conséquences sur les personnes (RGPD, CNIL)
Public	Nul	Aucune
Diffusion Limitée	Modéré	Les personnes concernées ne seront pas impactées ou pourraient connaitre **quelques désagréments, qu'elles surmonteront sans difficulté** (perte de temps pour réitérer des démarches ou pour attendre de les réaliser, agacement, énervement...).
Confidentiel	Important	
Diffusion Restreinte (II 901)	Catastrophique	

Exemple : RGPD

Niveau de classification	Impact	Conséquences sur les personnes (RGPD, CNIL)
Public	Nul	Aucune
Diffusion Limitée	Modéré	Les personnes concernées ne seront pas impactées ou pourraient connaitre **quelques désagréments, qu'elles surmonteront sans difficulté** (perte de temps pour réitérer des démarches ou pour attendre de les réaliser, agacement, énervement...).
Confidentiel	Important	Les personnes concernées pourraient connaitre des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés (frais supplémentaires, refus d'accès à des prestations commerciales, peur, incompréhension, stress, affection physique mineure...) ou de sérieuses difficultés (détournements d'argent, interdiction bancaire, dégradation de biens, perte d'emploi, assignation en justice, aggravation de l'état de santé...)
Diffusion Restreinte (II 901)	Catastrophique	

Exemple : RGPD

Niveau de classification	Impact	Conséquences sur les personnes (RGPD, CNIL)
Public	N	
Diffusion Limitée	M	
Confidentiel	Important	Les personnes concernées pourraient connaitre des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés (frais supplémentaires, refus d'accès à des prestations commerciales, peur, incompréhension, stress, affection physique mineure...) ou de sérieuses difficultés (détournements d'argent, interdiction bancaire, dégradation de biens, perte d'emploi, assignation en justice, aggravation de l'état de santé...)
Diffusion Restreinte (II 901)	Catastrophique	

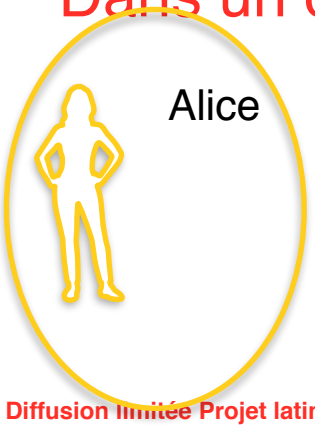
Les personnes concernées pourraient connaitre des désagréments significatifs, **qu'elles pourront surmonter malgré quelques difficultés** (frais supplémentaires, refus d'accès à des prestations commerciales, peur, incompréhension, stress, affection physique mineure...) **ou de sérieuses difficultés** (détournements d'argent, interdiction bancaire, dégradation de biens, perte d'emploi, assignation en justice, aggravation de l'état de santé...)

Exemple : RGPD

Niveau de classification	Impact	Conséquences sur les personnes (RGPD, CNIL)
Public	Nul	Aucune
Diffusion Limitée	Modéré	Les personnes concernées ne seront pas impactées ou pourraient connaitre **quelques désagréments, qu'elles surmonteront sans difficulté** (perte de temps pour réitérer des démarches ou pour attendre de les réaliser, agacement, énervement...).
Confidentiel	Important	Les personnes concernées pourraient connaitre des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés (frais supplémentaires, refus d'accès à des prestations commerciales, peur, incompréhension, stress, affection physique mineure...) ou de sérieuses difficultés (détournements d'argent, interdiction bancaire, dégradation de biens, perte d'emploi, assignation en justice, aggravation de l'état de santé...)
Diffusion Restreinte (II 901)	Catastrophique	Les personnes concernées pourraient connaitre des conséquences significatives, voire irrémédiables, **qu'elles pourraient ne pas surmonter** (péril financier tel que des dettes importantes ou une impossibilité de travailler, affection psychologique ou physique de longue durée, décès...)

☑ Vocabulaire commun

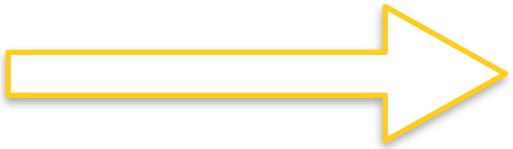
Dans un contexte RGPD



Diffusion limitée Projet latin

Nam tempus feugiat elit, vel tristique dolor. Vivamus sagittis augue ac eros tempor porttitor. Nam tempus lorem non nisi tempor, in mollis sapien lobortis. Praesent blandit quam nec purus venenatis laoreet.

Les personnes concernées pourraient connaitre quelques désagréments, qu'elles surmonteront sans difficulté



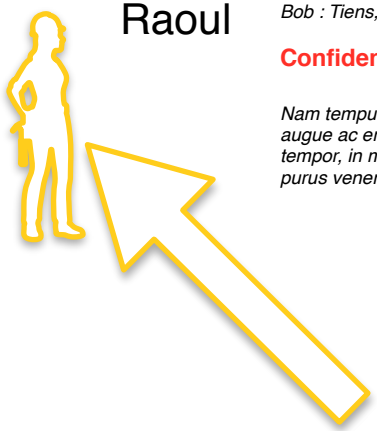
Bob

Diffusion limitée Projet latin

Nam tempus feugiat elit, vel tristique dolor. Vivamus sagittis augue ac eros tempor porttitor. Nam tempus lorem non nisi tempor, in mollis sapien lobortis. Praesent blandit quam nec purus venenatis laoreet.

Les personnes concernées pourraient connaitre quelques désagréments, qu'elles surmonteront sans difficulté

☑ Actions associées

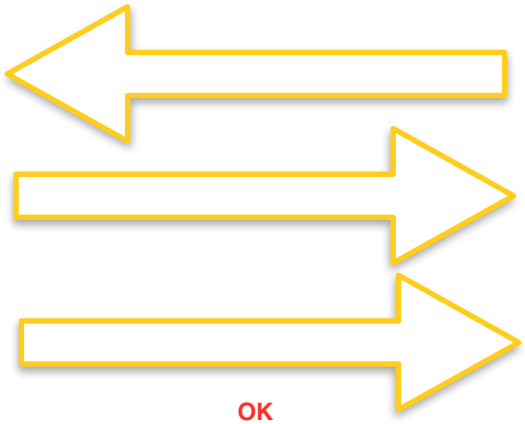


Bob : Tiens, regarde ce que m'envoie Alice

Confidentiel GT B+A

Nam tempus feugiat elit, vel tristique dolor. Vivamus sagittis augue ac eros tempor porttitor. Nam tempus lorem non nisi tempor, in mollis sapien lobortis. Praesent blandit quam nec purus venenatis laoreet.

Je souhaite transmettre à Raoul, parce qu'il a besoin de connaître cette information pour le traitement envisagé



Confidentiel Projet latin

Nam tempus feugiat elit, vel tristique dolor. Vivamus sagittis augue ac eros tempor porttitor. Nam tempus lorem non nisi tempor, in mollis sapien lobortis. Praesent blandit quam nec purus venenatis laoreet.

Les personnes concernées pourraient connaitre de sérieuses difficultés

Confidentiel Projet latin

Nam tempus feugiat elit, vel tristique dolor. Vivamus sagittis augue ac eros tempor porttitor. Nam tempus lorem non nisi tempor, in mollis sapien lobortis. Praesent blandit quam nec purus venenatis laoreet.

Les personnes concernées pourraient connaitre de sérieuses difficultés

À quoi ça sert ?

☑ Se donner un vocabulaire commun

☑ Décrire les actions associées à la classification d'une information


Marquage


Stockage / Sauvegarde


Affichage


Création


Impression


Fin de vie


Acheminement


Retransmission

Solution d'échange numérique

Contexte RGPD

Alice

Bob

Solution différente en fonction de la classification

Confidentiel Projet latin

Nam tempus feugiat elit, vel tristique dolor. Vivamus sagittis augue ac eros tempor porttitor. Nam tempus lorem non nisi tempor, in mollis sapien lobortis. Praesent blandit quam nec purus venenatis laoreet.

Confidentiel Projet latin

Nam tempus feugiat elit, vel tristique dolor. Vivamus sagittis augue ac eros tempor porttitor. Nam tempus lorem non nisi tempor, in mollis sapien lobortis. Praesent blandit quam nec purus venenatis laoreet.

Solution d'échange numérique

Une solution d'échange numérique c'est :

Un service + exposition au risque + utilisation de chiffrement de bout en bout

Skype, Google Hangout, Drive, appear.in, WhatsApp, Dropbox, Amazon, Microsoft Office 365 Cloud/Online, etc…

Grille d'analyse	Bon	Pas bon
Comment est opérée l'infrastructure ?		Ne sais pas
Quel est le niveau réel de confidentialité des échanges ?		Ne sais pas
Quelle est la gestion et l'exploitation des méta-données ?		Ne sais pas
Quel est le modèle économique de la plateforme ?		Ne sais pas
Est-ce qu'il y a des doutes raisonnables qu'un État étranger puisse accéder aux infos ?		Oui
Est-ce que la règlementation Européenne s'applique facilement ?		Non
L'opérateur est-il soumis à une réglementation nationale qui le contraint à donner accès aux informations, y compris stockées sur le territoire européen ?		Oui
Est-ce qu'Inria et l'opérateur ont des relations contractuelles ?		Non
Est-ce qu'Inria opère le service ou le fait opérer pour son compte ?		Non

Solutions Framasoft (framadate, framapad, framaforms, framatalk …)

Grille d'analyse	Bon	Pas bon
Comment est opérée l'infrastructure ?		Ne sais pas
Quel est le niveau réel de confidentialité des échanges ?		Ne sais pas
Quelle est la gestion et l'exploitation des méta-données ?	Conforme RGPD	
Quel est le modèle économique de la plateforme ?	Asso loi 1901	
Est-ce qu'il y a des doutes raisonnables qu'un État étranger puisse accéder aux infos ?	Non	
Est-ce que la règlementation Européenne s'applique facilement ?	Oui	
L'opérateur est-il soumis à une réglementation nationale qui le contraint à donner accès aux informations, y compris stockées sur le territoire européen ?	Non	
Est-ce qu'Inria et l'opérateur ont des relations contractuelles ?		Non
Est-ce qu'Inria opère le service ou le fait opérer pour son compte ?		Non

Solutions RENATER, solutions partenaires

Grille d'analyse	Bon	Pas bon
Comment est opérée l'infrastructure ?	On en a une bonne idée (et on peut demander)	
Quel est le niveau réel de confidentialité des échanges ?	Idem	
Quelle est la gestion et l'exploitation des méta-données ?	Conforme RGPD	
Quel est le modèle économique de la plateforme ?	État, relation contractuelle	
Est-ce qu'il y a des doutes raisonnables qu'un État étranger puisse accéder aux infos ?	Non	
Est-ce que la règlementation Européenne s'applique facilement ?	Oui	
L'opérateur est-il soumis à une réglementation nationale qui le contraint à donner accès aux informations, y compris stockées sur le territoire européen ?	Non	
Est-ce qu'Inria et l'opérateur ont des relations contractuelles ?	Oui	
Est-ce qu'Inria opère le service ou le fait opérer pour son compte ?		Non

Solutions Inria ou opérées pour le compte d'Inria

Grille d'analyse	Bon	Pas bon
Comment est opérée l'infrastructure ?	On sait	
Quel est le niveau réel de confidentialité des échanges ?	On sait	
Quelle est la gestion et l'exploitation des méta-données ?	Aucune	
Quel est le modèle économique de la plateforme ?	Nous payons	
Est-ce qu'il y a des doutes raisonnables qu'un État étranger puisse accéder aux infos ?	Non	
Est-ce que la règlementation Européenne s'applique facilement ?	Oui	
L'opérateur est-il soumis à une réglementation nationale qui le contraint à donner accès aux informations, y compris stockées sur le territoire européen ?	Non	
Est-ce qu'Inria et l'opérateur ont des relations contractuelles ?	Oui	
Est-ce qu'Inria opère le service ou le fait opérer pour son compte ?	Oui	

Exemples

Infrastructure / Service	Chiffrement	Confiance	Utilisation max
Google Drive, Dropbox, Amazon, Office 365 Cloud/Online	Sans	Faible	Public
	Avec	Moyenne	Diffusion limitée
FileSender de RENATER	Sans	Moyenne	Diffusion limitée
	Avec	Très importante	Tous
Rendez-vous de RENATER	Sans	Moyenne	Diffusion limitée
Partage (Système de gestion de contenu Inria à base d'Alfresco)	Sans	Moyenne	Diffusion limitée
	Avec	Très importante	Tous
MyBox (Solution Inria à base de Seafile)	Sans	Moyenne	Diffusion limitée
	Avec *	Très importante	Tous
Serveur de fichiers Inria, non accessible directement depuis Internet	Sans	Importante	Confidentiel
	Avec	Très importante	Tous

* Librairie chiffrée et DD poste du travail chiffré

Merci

Didier Benza
FSD d'Inria