SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]

La Protection des Données à caractère Personnelles [P.D.P.]

Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers

TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

De la *S.S.I.* à la *P.D.P.* : convergences / divergences

[Sécurisation des Systèmes d'Information** versus **Protection des Données Personnelles]

Brefs historiques : les ***origines de la S.S.I.*** & la ***genèse de la P.D.P.***

*Détour par la **'dependability'** :* ***'reliability' + 'maintainability' + 'safety' + …***
[ou "sûreté-de-fonctionnement"] ***… + 'availability' & 'integrity & 'confidentiality'***

*Différenciation entre les **3-Sécurités** :* ***S-immunité, S-innocuité, S-intimité***

*Référentiels de **bonnes pratiques** :* ***ISO-IEC27xxx, DO178b, R.G.P.D.***

*Principes génériques de **S-immunité [S.S.I.]** :* ***'Security-by-Design'*** & ***'Security-by-Default'***
*Principes génériques de **S-intimité [P.D.P.]** :* ***'Privacy-by-Design'*** & ***'Privacy-by-Default'***

*Principales **convergences** entre **S.S.I.** et **P.D.P.** :* ***Politique S.S.I., Politique P.D.P.***
*Principales **divergences** entre **S.S.I.** et **P.D.P.** :* le ***R.S.S.I.***, le ***D.P.D./D.P.O.***

Conclusion ***"Qui (S.S.I./P.D.P.) est au service de l'autre (P.D.P./S.S.I.) ?"***

Gilles TROUESSIN – ***A.C.C.E.S.S.S.-I.F.*** – *+33(0)6.63.10.50.76 – gilles.trouessin@orange.fr*

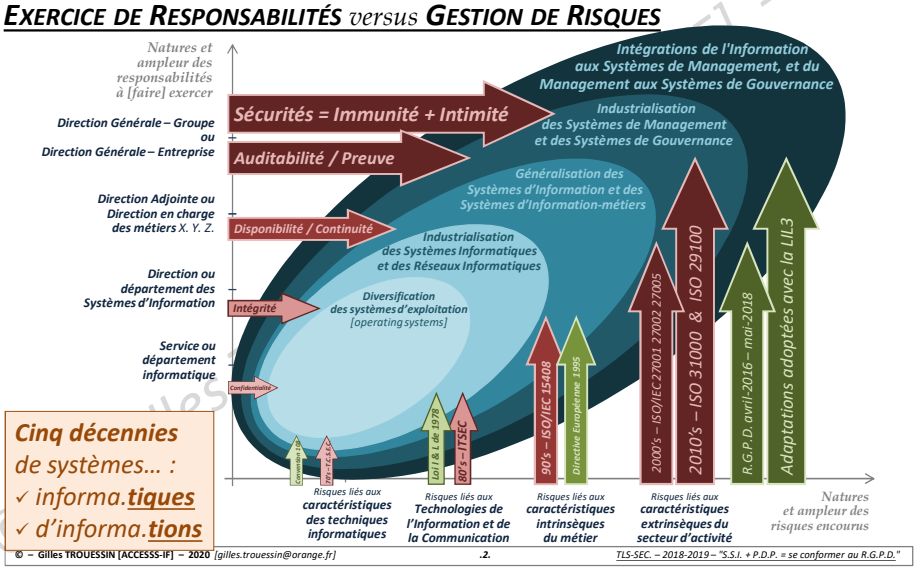
SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]

La Protection des Données à caractère Personnelles [P.D.P.]

Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers

TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

EXERCICE DE RESPONSABILITÉS *versus* ***GESTION DE RISQUES***



Cinq décennies *de systèmes… :*
✓ *informa.**tiques***
✓ *d'informa.**tions***

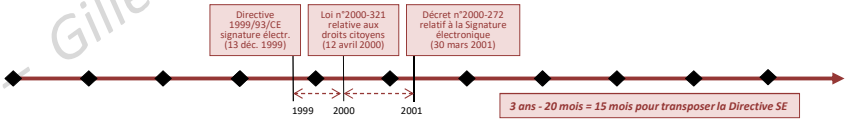
© – Gilles TROUESSIN [ACCESSS-IF] – 2020 [gilles.trouessin@orange.fr] .2. TLS-SEC. – 2018-2019 – "S.S.I. + P.D.P. = se conformer au R.G.P.D."

Une illustration assez frappante

Comparaison chronologique : *P.D.P.* vs. Signature Électronique

- Loi originelle « *Informatique & Libertés* » du **06 janvier 1978**, révision majeure du **06 août 2004**
- *Directive européenne* du **24 octobre 1995**, abrogée par le *Règlement n°2016/679* du **27 avril 2016**

- *Directive européenne 1999/93/CE*, du **13 déc. 1999** (cadre communautaire pour les signatures. électronique)
- *Loi n°2000-321* du **12 avril 2000** (relative aux droits des citoyens dans leurs relations avec les administration)
- *Décret n°2001-272* du **30 mars 2001** (objectif 1316-4 du code civil et relatif à la signature électronique)



SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]
La Protection des Données à caractère Personnelles [P.D.P.]
Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers
TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

SENSIBILISATION AUX ENJEUX DE LA PROTECTION DES D.C.P.

Genèse & Historique */ Principes génériques & ... Acteurs & Responsabilités*

En guise de rappels

Loi(s) Informatique et libertés [LIL]

- **Loi n°78-17 originelle du 6 janvier 1978**
  - Loi originelle relative *à l'informatique aux fichiers et aux libertés*
  - Responsable / finalité des traitements et surtout principe de consentement
  - *Obligation d'information* (lors de la collecte d'information) et Droit d'accès / droit de rectification / droit de suppression
- **Loi n°78-17 modifiée du 6 août 2004**
  - Loi modifiée relative *à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* et modifiant la loi de 1978
  - CPDCP – Correspondant à la Protection des Données à Caractère Personnel ou *CIL désigné* – Correspondant Informatique et Libertés
  - *Homologation de produits et services* de protection des données personnelles
  - *Pouvoirs étendus* de la CNIL / nouveau *pouvoir de sanction* autonome
- **La loi n° 2018-493 du 20 juin 2018 & ordonnance 2018-1125 du 12 décembre 2018**
  - promulguée le 21 **juin 2018** et modifie la **loi Informatique et Libertés**…
  - … afin de mettre en conformité le **droit national** avec le **cadre juridique européen**

SENSIBILISATION AUX ENJEUX DE LA PROTECTION DES D.C.P.

***Genèse & Historique** / Principes génériques & ...de base / Acteurs & Responsabilités*

Autres rappels

Directive Européenne vs. Règlement Européen

❑ **Directive européenne 95/46/CE de 1995**
- ❖ Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la ***protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données***
- ❖ Principes de proportionnalité, de transparence et de finalité légitime
- ❖ La ***Commission Nationale de l'Informatique et des Libertés (C.N.I.L.)*** en tant que modèle pour les ***autorités de protection des données personnelles***e

❑ **Règlement européen 2016/679 de 27 avril 2016**
- ❖ Relatif à la protection des personnes physiques à l'égard du ***traitement des données à caractère personnel*** et à ***la libre circulation de ces données***, et abrogeant la directive 95/46/CE ; révision de la directive de 1995 par ce règlement 2016 visant à apporter :
  - ➢ *un allégement des formalités préalables pesant sur les entreprises,*
  - ➢ *un renforcement des **droits du citoyen**,*
  - ➢ *une harmonisation des **pouvoirs et des compétences des autorités de contrôle**,*
  - ➢ *une coopération renforcée **entre les autorités***
- ❖ Généralisation du ***CIL via le nouveau DPO*** (Délégué à la Protection des Données)
- ❖ Pouvoir de ***sanction*** (jusqu'à 4% du chiffre d'affaires ou 20 M€) / ***Droit à « l'oubli »*** / ***Portabilité***

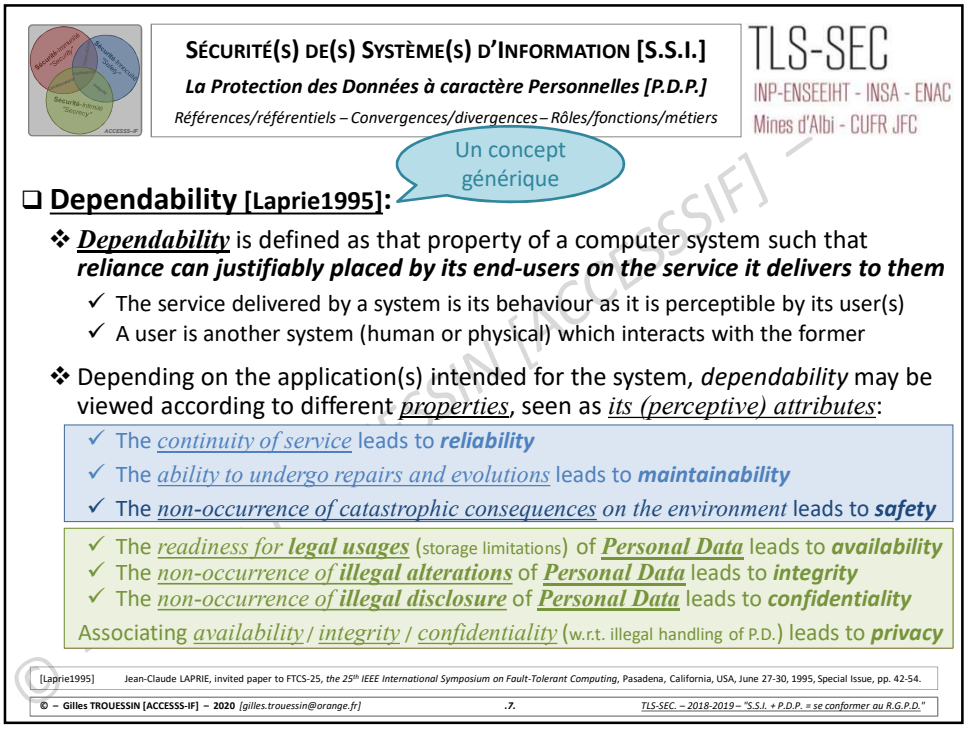
SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]
La Protection des Données à caractère Personnelles [P.D.P.]
Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers
TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

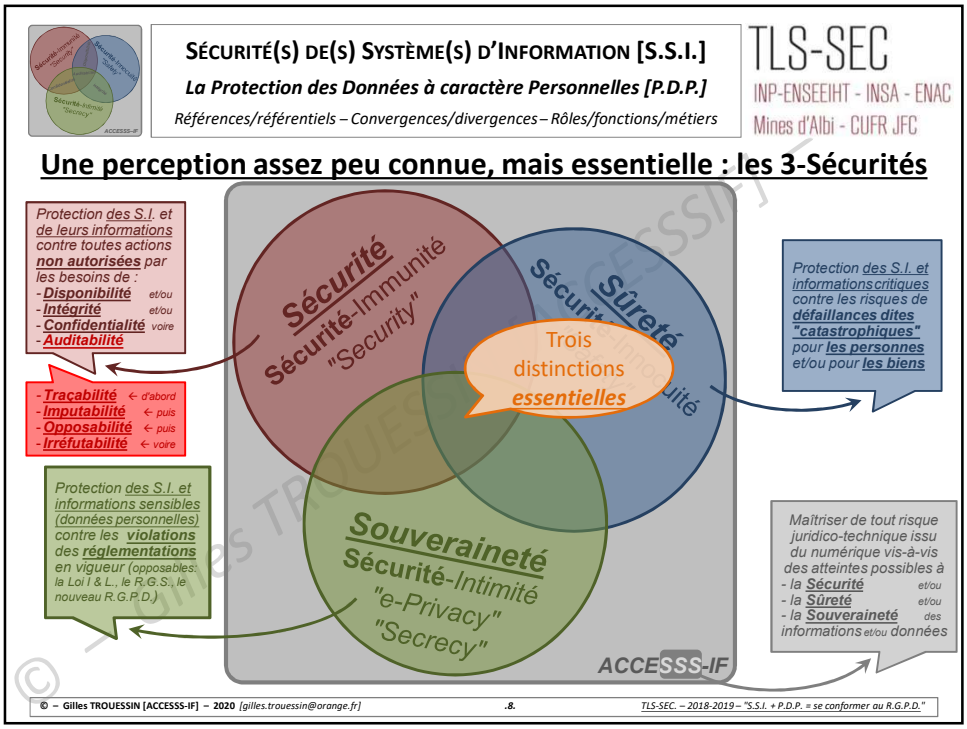
❑ ***Rappels juridiques :*** **protection des Données à Caractère Personnel**
- ❖ Long historique en France (en particulier) et en Europe (en général)
- ❖ Partie intégrante du respect de la vie privée des Personnes Concernées et contribuant au respect des droits fondamentaux des personnes physiques

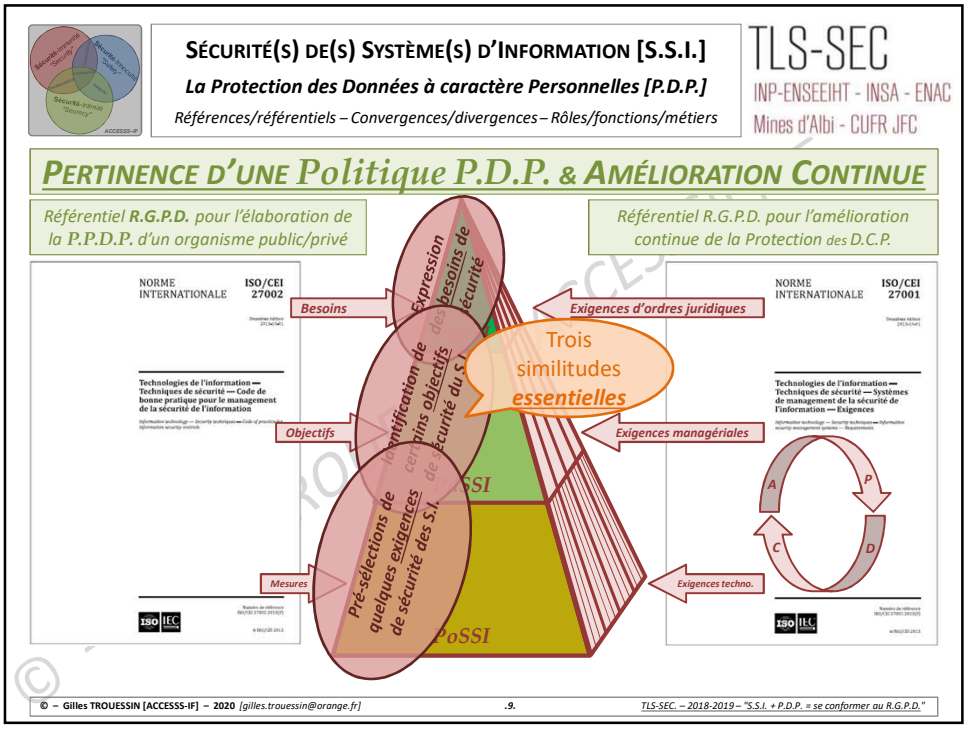
❑ ***Un long historique français :*** **obligation de conformité à la *"Loi I & L"***
- ❖ Loi *Informatique & Libertés* de 1978, révisée en 2004 et re-révisée en 2018
- ❖ D'abord intitulée : *« loi relative à l'informatique, aux fichiers et aux libertés »* et désormais intitulée : *« loi relative à la protection des personnes physiques à l'égard des traitements de données personnelles (et modifiant la loi de 1978) »*

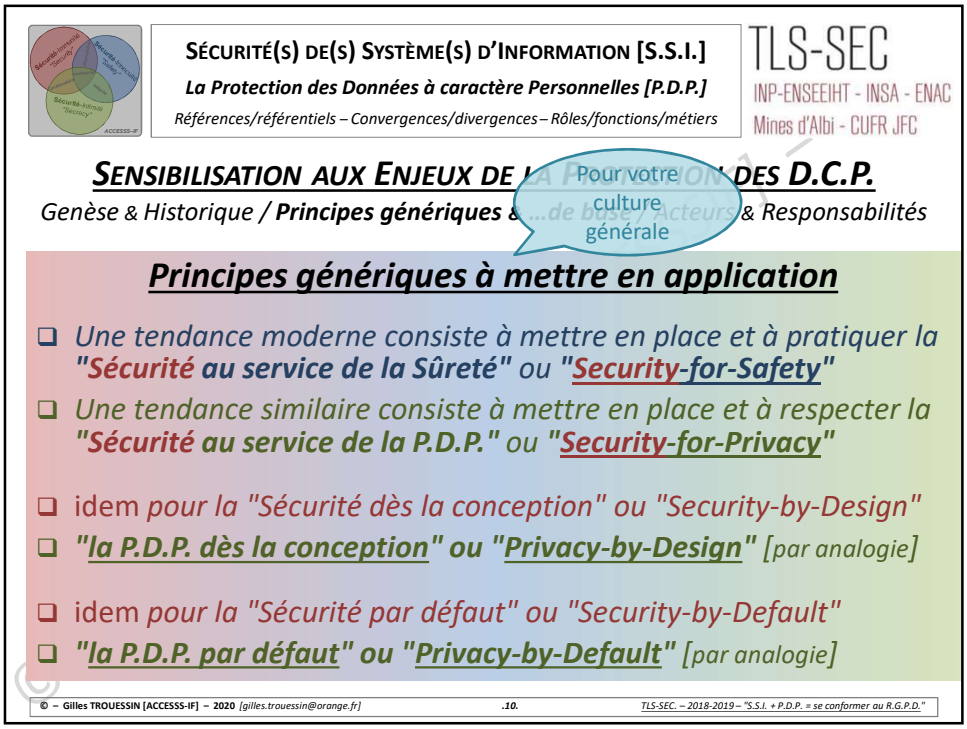
❑ ***Réglementation Européenne :*** **le RGPD remplace la Directive de 1995**
- ❖ Depuis le *04 mai 2016*, le *RGPD* était applicable intégralement (mais facultatif) mais, depuis le *25 mai 2018*, il est d'application impérative et en intégralité
- ❖ L'obligation d'application du règlement *RGPD* est à compléter par l'application de la récente loi adaptative « Informatique & Libertés » du 20 juin 2018

Nota : **voir en annexe pour de plus amples détails sur la genèse de la "Loi I & L" et sur les origines du *RGPD*.**


SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]
La Protection des Données à caractère Personnelles [P.D.P.]
Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers
TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC
Un concept générique
Dependability [Laprie1995]:
Dependability is defined as that property of a computer system such that reliance can justifiably placed by its end-users on the service it delivers to them
The service delivered by a system is its behaviour as it is perceptible by its user(s)
A user is another system (human or physical) which interacts with the former
Depending on the application(s) intended for the system, dependability may be viewed according to different properties, seen as its (perceptive) attributes:
The continuity of service leads to reliability
The ability to undergo repairs and evolutions leads to maintainability
The non-occurrence of catastrophic consequences on the environment leads to safety
The readiness for legal usages (storage limitations) of Personal Data leads to availability
The non-occurrence of illegal alterations of Personal Data leads to integrity
The non-occurrence of illegal disclosure of Personal Data leads to confidentiality
Associating availability / integrity / confidentiality (w.r.t. illegal handling of P.D.) leads to privacy
[Laprie1995] Jean-Claude LAPRIE, invited paper to FTCS-25, the 25th IEEE International Symposium on Fault-Tolerant Computing, Pasadena, California, USA, June 27-30, 1995, Special Issue, pp. 42-54.
© – Gilles TROUESSIN [ACCESSS-IF] – 2020 [gilles.trouessin@orange.fr] .7. TLS-SEC. – 2018-2019 – "S.S.I. + P.D.P. = se conformer au R.G.P.D."


SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]
La Protection des Données à caractère Personnelles [P.D.P.]
Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers
TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC
Une perception assez peu connue, mais essentielle : les 3-Sécurités
Protection des S.I. et de leurs informations contre toutes actions non autorisées par les besoins de :
- Disponibilité et/ou
- Intégrité et/ou
- Confidentialité voire
- Auditabilité
- Traçabilité ← d'abord
- Imputabilité ← puis
- Opposabilité ← puis
- Irréfutabilité ← voire
Protection des S.I. et informations sensibles (données personnelles) contre les violations des réglementations en vigueur (opposables: la Loi I & L., le R.G.S., le nouveau R.G.P.D.)
Sécurité
Sécurité-Immunité
"Security"
Sûreté
Sécurité-Intégrité
"Safety"
Souveraineté
Sécurité-Intimité
"e-Privacy"
"Secrecy"
Trois distinctions essentielles
ACCESSS-IF
Protection des S.I. et informations critiques contre les risques de défaillances dites "catastrophiques" pour les personnes et/ou pour les biens
Maîtriser de tout risque juridico-technique issu du numérique vis-à-vis des atteintes possibles à
- la Sécurité et/ou
- la Sûreté et/ou
- la Souveraineté des informations et/ou données
© – Gilles TROUESSIN [ACCESSS-IF] – 2020 [gilles.trouessin@orange.fr] .8. TLS-SEC. – 2018-2019 – "S.S.I. + P.D.P. = se conformer au R.G.P.D."


SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]
La Protection des Données à caractère Personnelles [P.D.P.]
Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers
TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC
PERTINENCE D'UNE Politique P.D.P. & AMÉLIORATION CONTINUE
Référentiel R.G.P.D. pour l'élaboration de la P.P.D.P. d'un organisme public/privé
Référentiel R.G.P.D. pour l'amélioration continue de la Protection des D.C.P.
NORME INTERNATIONALE ISO/CEI 27002
Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information
NORME INTERNATIONALE ISO/CEI 27001
Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences
Besoins
Objectifs
Mesures
Exigences d'ordres juridiques
Exigences managériales
Exigences techno.
Expression des besoins de sécurité
Identification de certains objectifs de sécurité du S.I.
Pré-sélections de quelques exigences de sécurité des S.I.
SSI
PoSSI
Trois similitudes essentielles
P
D
C
A
© – Gilles TROUESSIN [ACCESSS-IF] – 2020 [gilles.trouessin@orange.fr] .9. TLS-SEC. – 2018-2019 – "S.S.I. + P.D.P. = se conformer au R.G.P.D."


SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]
La Protection des Données à caractère Personnelles [P.D.P.]
Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers
TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC
SENSIBILISATION AUX ENJEUX DE LA PROTECTION DES D.C.P.
Pour votre culture générale
Genèse & Historique / Principes génériques & ...de base / Acteurs & Responsabilités
Principes génériques à mettre en application
Une tendance moderne consiste à mettre en place et à pratiquer la "Sécurité au service de la Sûreté" ou "Security-for-Safety"
Une tendance similaire consiste à mettre en place et à respecter la "Sécurité au service de la P.D.P." ou "Security-for-Privacy"
idem pour la "Sécurité dès la conception" ou "Security-by-Design"
"la P.D.P. dès la conception" ou "Privacy-by-Design" [par analogie]
idem pour la "Sécurité par défaut" ou "Security-by-Default"
"la P.D.P. par défaut" ou "Privacy-by-Default" [par analogie]
© – Gilles TROUESSIN [ACCESSS-IF] – 2020 [gilles.trouessin@orange.fr] .10. TLS-SEC. – 2018-2019 – "S.S.I. + P.D.P. = se conformer au R.G.P.D."

❑ ***Principe de « protection dès la conception » : "Privacy-by-Design"***

❖ *Définition :*

« …Afin d'être en mesure de démontrer qu'il respecte le présent règlement, le responsable du traitement devrait adopter des règles internes et mettre en œuvre des mesures qui respectent, en particulier, les principes de protection des données dès la conception et de protection des données par défaut. »

❖ *Explication :*

Faire en sorte de prendre en compte la protection des *D.C.P.* au plus tôt dans le cycle de vie d'un projet, d'un logiciel / progiciel / etc.

❖ *Justification(s) :*

Plus tôt les spécifications (contraintes) liées à la protection des *D.C.P.* seront exprimées et traitées ; *plus facile sera leur prise en compte…*

Plus tôt les spécifications (contraintes) liées à la protection des *D.C.P.* seront exprimées et traitées ; *moins coûteuse sera leur intégration…*

❖ *Illustration(s) :*

Définir au plus tôt, qui peut accéder aux *D.C.P.*, pourquoi et pour quoi faire ; et donc les profils d'accès autorisés (cf. *"limitation des finalités"*)

❑ ***Principe de « protection par défaut » : ou "Privacy-by-Default"***

❖ *Définition :*

« …Afin d'être en mesure de démontrer qu'il respecte le présent règlement, le responsable du traitement devrait adopter des règles internes et mettre en œuvre des mesures qui respectent, en particulier, les principes de protection des données dès la conception et de protection des données par défaut. »

❖ *Explication :*

Faire en sorte de prendre en compte, implicitement, en priorité, la protection les intérêts de la personne concerné et donc celle de leurs *D.C.P.*

❖ *Justification(s) :*

Si la protection des *D.C.P.* est la règle par défaut, alors bon nombre de *risques de violation de celles-ci seront éliminés à la source…*

De plus, en appliquant systématiquement ce principe, ce "réflexe" fera partie de la *démarche normale de conception des systèmes d'information*

❖ *Illustration(s) :*

S'il n'est pas justifié d'accéder à telle ou telle donnée personnelle, alors il faut par défaut en interdire l'utilisation (cf. *"minimisation des données"*)

SENSIBILISATION AUX ENJEUX DE LA PROTECTION DES D.C.P.

*Genèse & Historique / **Principes génériques & …de base** / Acteurs & Responsabilités*

Définitions de base essentielles [article #4]

- ***« donnée à caractère personnel »*** *(…se rapportant à une personne identifiée/identifiable)*
- ***« traitement »*** *(…acception du terme "traitement" au sens le plus large)*
- ***« pseudonymisation »*** *(…nuance importante avec "anonymisation")*
- ***« fichier »*** *(…acception du terme "fichier" au sens le plus large)*

Des notions de base qui sont ***essentielles***

- ***« personne physique identifiable** [data subject]* ***»*** *(…personne concernée par la D.C.P.)*
- ***« responsable du traitement** [controller]* ***»*** *(…fondement de mise en œuvre du R.G.P.D.)*
- ***« sous-traitant** [processor]* ***»*** *(…autre fondement essentiel de mise en œuvre du R.G.P.D.)*
- ***« destinataire »*** *(…entité qui peut être 'destinataire' de donnée à caractère personnel)*
- ***« tiers »*** *(…entité autre que la personnes concernée, le R.T., le S.T. ou le D.P.D.)*

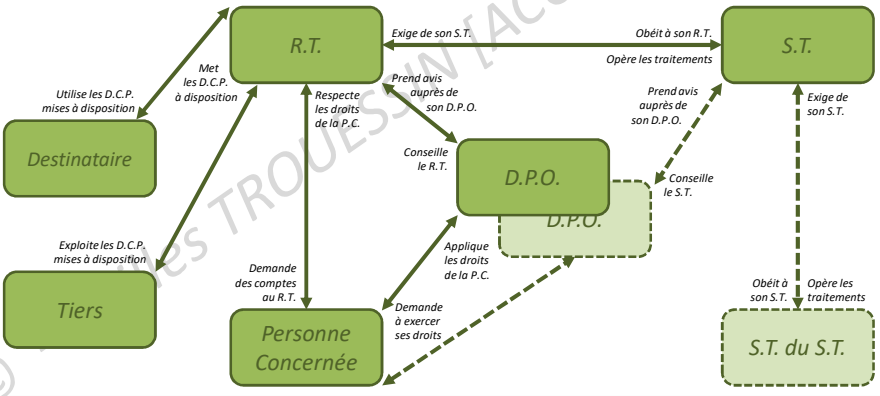
- ***« délégué à la protection des données »*** *(…principal facilitateur de conformité au R.G.P.D.)*
- ***« autorité de contrôle (concernée) »*** *(…autorité publique indépendante [compétente])*

← ***Notions essentielles*** **sur lesquelles repose la conformité au *R.G.P.D.***
(…et la preuve des *mise-et-maintien en conformité* vis-à-vis du *R.G.P.D.*)

SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]
La Protection des Données à caractère Personnelles [P.D.P.]
Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers
TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

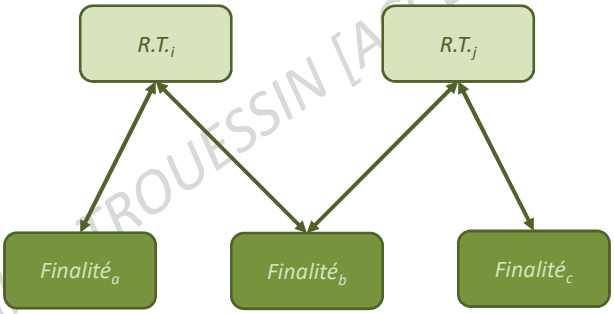
❑ *Schématisation ➔ relations entre les différents types d'acteurs*

- ❖ *R.T.* ⇔ *S.T.* et aussi *R.T.* ⇔ *D.P.O.* ou encore *S.T.* ⇔ *D.P.O.*
- ❖ *R.T.* ⇔ *Personne Concernée* et aussi *D.P.O.* ⇔ *Personne Concernée*
- ❖ *R.T.* ⇔ *Destinataire* et aussi *R.T.* ⇔ *Tiers*



❑ ***Schématisation ➔ particularité de la responsabilité conjointe***

- ❖ $R.T._i \Leftrightarrow R.T._j$
- ❖ $Finalité_a \Leftrightarrow Finalité_b \Leftrightarrow Finalité_c$



SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]
La Protection des Données à caractère Personnelles [P.D.P.]
Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers
TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

❑ ***Le « Responsable du Traitement [R.T.] »***

- ❖ *Intitulé :*
  « "responsable du traitement", la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre. [Art. 4] »
- ❖ *Explication :*
  Le *Responsable du Traitement* est l'entité pour le compte de laquelle est réalisé le traitement des *D.C.P.* concernées
- ❖ *Justification(s) :*
  La version anglaise du *R.G.P.D.* dénomme le *Responsable du Traitement*, *"the Controller"*, au sens où le traitement de *D.C.P.* doit être sous son contrôle
- ❖ *Illustration(s) :*
  Une mutuelle, faisant procéder au paiement, en faveur d'un de ses adhérents, à titre du remboursement complémentaire de frais de soins de santé avancés, est alors considéré comme le *Responsable de ce Traitement "remboursement"*

❑ *Principe spécifique de « responsabilité [du R.T.] »*

❖ *Intitulé :*
« Le responsable du traitement est responsable du respect du paragraphe 1 [n.d.l.r. toutes les propriétés énumérées précédemment : licéité/loyauté/..., intégrité/confidentialité]
et est en mesure de démontrer que celui- ci est respecté (cf. responsabilité). »

❖ *Explication :*
Le *Responsable du Traitement* est l'acteur principal du respect de la *Personne Concernée* et, donc, l'artisan essentiel de la conformité vis-à-vis du *R.G.P.D.*

❖ *Justification(s) :*
Puisque le traitement de *D.C.P.* doit rester sous son contrôle (cf. *"Controller"*), le *Responsable du Traitement* est le seul à pouvoir se porter garant du respect des *D.C.P.* traitées (directement) et des *Personnes Concernées* (indirectement)

❖ *Illustration(s) :*
Cette même mutuelle est redevable de respecter les obligations qui incombent à un *Responsable du Traitement*, pour ce traitement *"remboursement"* ; et elle est également redevable de fournir la preuve du respect de ces obligations

SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]
La Protection des Données à caractère Personnelles [P.D.P.]
Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers
TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

❑ *Le « Sous-Traitant [S.T.] »*

❖ *Intitulé :*
« "sous-traitant", la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. [Art. 4] »

❖ *Explication :*
Le *Sous-Traitant* est l'entité qui opère le traitement pour le compte d'une entité qui lui a confié la réalisation du traitement (i.e., le *Responsable du Traitement*)

❖ *Justification(s) :*
La version anglaise du *R.G.P.D.* dénomme le *Sous-Traitant*, *"the Processor"*, au sens où le traitement des *D.C.P.* doit être opéré par ses soins

❖ *Illustration(s) :*
Cette même mutuelle, faisant procéder au remboursement de ses adhérents, en confiant le traitement *"remboursement"* à une entité qui gère ses bases de données et opère les flux financiers de remboursement, ordonne de fait à son *Sous-Traitant* d'effectuer les opérations financières de remboursements

SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]

La Protection des Données à caractère Personnelles [P.D.P.]

Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers

TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

❑ ***Responsabilité du « Sous-Traitant [S.T.] »***

❖ *Intitulé :*

« Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée. [Art. 28] »

❖ *Explication :*

Le *Sous-Traitant* est aux ordres du *Responsable du Traitement* ; il est, donc, l'opérateur garant de la mise en œuvre de moyens conformes au *R.G.P.D.*

❖ *Justification(s) :*

Le *Responsable du Traitement,* ayant sous contrôle le traitement des *D.C.P.*, demande au *Sous-Traitant* de mettre en œuvre les moyens pour respecter les *D.C.P.* traitées (directement) et les *Personnes Concernées* (indirectement)

❖ *Illustration(s) :*

L'entité, à qui la mutuelle confie l'exploitation du traitement *"remboursement"*, doit garantir le bon traitement (sécurité) des bonnes données (intégrité)

SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]

La Protection des Données à caractère Personnelles [P.D.P.]

*Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers

TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

❑ ***Le « Délégué à la Protection des Données [D.P.D. / D.P.O.] »***

❖ *Intitulé :*

Cf. *« Article 37 – Désignation du Délégué à la Protection des Données »*
Cf. *« Article 38 – Fonction du Délégué à la Protection des Données »*
Cf. *« Article 39 – Missions du Délégué à la Protection des Données »*

❖ *Explication :*

Le *D.P.D./D.P.O.* est à voir comme le facilitateur, après de son *R.T.*, son *S.T.*, de la mise-et-maintien du traitement de *D.C.P.* en conformité avec le *R.G.P.D.*

❖ *Justification(s) :*

« Le responsable du traitement et le sous-traitant veillent à ce que le délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des D.C.P. [Art. 38] »

❖ *Illustration(s) :*

« Les missions du D.P.D. sont de […] informer et conseiller, […] de contrôler, […] de dispenser des conseils sur demande (cf. E.I.V.P., E.I.P.D., D.P.I.A.) et […] de faire office de point de contact vis-à-vis de l'autorité de contrôle (CNIL) »

SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]

La Protection des Données à caractère Personnelles [P.D.P.]

Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers

TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

❑ ***Responsabilité du « Délégué à la Protection des Données [D.P.O.] »***

❖ *Intitulé :*

Cf. *« Article 37 – Désignation du Délégué à la Protection des Données »*
Cf. *« Article 38 – Fonction du Délégué à la Protection des Données »*
Cf. *« Article 39 – Missions du Délégué à la Protection des Données »*

❖ *Explication :*

Le *D.P.D./D.P.O.* est redevable d'apporter, à son *R.T.* ou *S.T.*, tout éclairage utile et pertinent pour la mise-et-maintien de tout traitement de toute *D.C.P.*, en conformité avec le *R.G.P.D.*

❖ *Justification(s) :*

Il n'exempte pas le *R.T.* de l'obligation de conformité du traitement de *D.C.P.* ; il n'exempte pas le *S.T.* de l'obligation de les opérer en conformité au *R.G.P.D.*

❖ *Illustration(s) :*

La mutuelle doit faire opérer un *"remboursement"* en conformité au *R.G.P.D.* ; l'opérateur du *"remboursement"* l'opère conformément à l'exigence *R.G.P.D.* ; et le *D.P.D./D.P.O.* apporte ses conseils pour facilité le maintien en conformité

SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]

La Protection des Données à caractère Personnelles [P.D.P.]

Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers

TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

❑ ***La notion de « Destinataire (des Données) »***

❖ *Intitulé :*

« "destinataire", la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires ; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement. [Art. 4] »

❖ *Explication :*

Un *Destinataire* est une entité susceptible de recevoir communication de *D.C.P.* Un *Destinataire* peut être un *Tiers* ; certaines *Autorités Publiques* ne le sont pas

❖ *Justification(s) :*

Vis-à-vis du registre des activités de traitement, il faut absolument identifier les destinataires, pour être en capacité de déterminer si le traitement est conforme

❖ *Illustration(s) :*

Si la *Caisse d'Assurance Maladie* est exclue des destinataires du traitement *"remboursement"*, alors aucune finalité ne doit prévoir d'y envoyer une copie

❑ *La notion de « Tiers »*

❖ *Intitulé :*
*« "tiers", une personne physique ou morale, une autorité publique, un service ou un organisme **autre que** la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel. [Art. 4] »*

❖ *Explication :*
Un *Tiers* ne peut donc être, ni le *R.T.*, ni le *S.T.*, ni la *Personne Concernée*, ni une personne placée sous l'autorité du *R.T.* ou placée sous l'autorité du *S.T.*

❖ *Justification(s) :*
Un *Tiers* est une entité autre que toute partie prenante du traitement de *D.C.P.* considéré : ni la *Personne Concernée* (elle-même), ni le *R.T.* (ou quiconque placé sous son autorité), ni le *S.T.* (ou quiconque placé sous son autorité)

❖ *Illustration(s) :*
Si la mutuelle adresse l'avis de paiement du remboursement de frais de santé à son adhérent (pour le compte de soins pour son enfant un mineur), alors le mineur est la *Personne Concernée* et son parent un *Tiers* vis-à-vis de celui-ci

SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]
La Protection des Données à caractère Personnelles [P.D.P.]
Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers
TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

SENSIBILISATION AUX ENJEUX DE LA PROTECTION DES D.C.P.

***Genèse & Historique** / Principes génériques & …de base / Acteurs & Responsabilités*

Fondements généraux à [faire] respecter

- ❑ ***L'obligation d'information de la personne concernée***
- ❑ ***Respect de la vie privée et libre circulation de biens/personnes***
- ❑ ***Les droits fondamentaux accordés à la personne concernée***
- ❑ ***Le libre exercice de ses droits, par la personne concernée***
- ❑ ***Les obligations faites au responsable de traitement***
- ❑ ***Les obligations faites au sous-traitant** [relativement nouveau]*
- ❑ ***Les missions confiées au délégué…** [partiellement nouveau]*
- ❑ ***Etc.***

Des fondements ***qui sont tous contraignants***

SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]

La Protection des Données à caractère Personnelles [P.D.P.]

Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers

TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

SENSIBILISATION AUX ENJEUX DE P… D.C.P.

Genèse & Historique / Principes génériques & …de base / Acteurs & Responsabilités

Pour mémoire : les *10* principes de base

Principes de base à mettre en application

1. ***Licéité, loyauté et transparence*** *(…pour l'exploitation de D.C.P.)*
2. ***Limitation des finalités*** *(…de tout traitement de D.C.P.)*
3. ***Minimisation des données*** *(…à caractère personnel manipulées)*
4. ***Exactitude des données*** *(souvent associée à… exhaustivité/fiabilité)*
5. ***Limitation de la conservation*** *(…limitation des durées de traitement)*
6. ***Intégrité et confidentialité*** *(…mesures techniques/organisationnelles)*

➔ ***Responsabilité*** **du responsable du traitement**
(…et preuve de sa responsabilité : obligation constante de ***"accountability"***)

SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]

La Protection des Données à caractère Personnelles [P.D.P.]

Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers

TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

❑ ***Principes spécifiques de « licéité / loyauté / transparence » :***

- ❖ *Intitulé :*
  « …traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) »
- ❖ *Explication :*
  Ces principes obligent le *Responsable du Traitement* à respecter les *D.C.P.* ;
  et, par conséquent, à respecter les personnes concernées par ces *D.C.P.*
- ❖ *Justification(s) :*
  Par définition, ces principes interdisent au *Responsable du Traitement [R.T.]* d'utiliser de manière abusive les *D.C.P.* qui lui ont été confiées, en :
  - ✓ N'effectuant que des traitements légitimement autorisés (cf. *"licéité"*)
  - ✓ Respectant ses propres engagements vis-à-vis des *D.C.P.* (cf. *"loyauté"*)
  - ✓ Permettant à la *Personne Concernée* d'en avoir connaissance (cf. *"transparence"*)
- ❖ *Illustration(s) :*
  Avant toute décision de traitement de *D.C.P.* il faut instruire le questionnement suivant : *« est-il licite / illicite d'effectuer tel traitement sur telle D.C.P. ? »*

SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]

La Protection des Données à caractère Personnelles [P.D.P.]

Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers

TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

❑ ***Principe spécifique de « limitation des finalités [du traitement] » :***

- ❖ *Intitulé :*
  « …collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités) ; »
- ❖ *Explication :*
  Conséquence directe des principes de *"licéité"*, *"loyauté"* et *"transparence"*
- ❖ *Justification(s) :*
  Afin d'être sûr d'avoir des traitement licites et loyaux, il faut formuler, sinon formaliser, les motifs (finalités) qui amènent à traiter telles ou telles *D.C.P.*
- ❖ *Illustration(s) :*
  Si certaines *D.C.P.* sont nécessaires à un traitement de type *R.H.*, il n'est pas pour autant normal de les utiliser, AUSSI, pour un traitement de type *"santé"*

SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]

La Protection des Données à caractère Personnelles [P.D.P.]

Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers

TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

❑ ***Principe spécifique de « limitation de la [durée de] conservation » :***

- ❖ *Intitulé :*
  « …conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation) ; »
- ❖ *Explication :*
  Ceci est à considérer conjointement avec le droit de retirer son consentement
- ❖ *Justification(s) :*
  Cela permet à la *Personne Concernée* de ne pas être liée indéfiniment au *Responsable du Traitement*
- ❖ *Illustration(s) :*
  Après avoir définitivement quitté une mutuelle, la *Personne Concernée* doit pouvoir être libérée de toute contrainte vis-à-vis de celle-ci

❑ ***Principe spécifique de « minimisation des données » :***

- *Intitulé :*
  « … adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ; »
- *Explication :*
  Minimiser les *D.C.P.* manipulables au titre d'un traitement permet d'éviter tout risque d'autre utilisation, potentiellement abusive, de ces mêmes *D.C.P.*
- *Justification(s) :*
  Le respect, conjointement, des deux principes de *i) limitation des finalités* et de *ii) minimisation des données*, permet de sécuriser l'utilisation correcte, et donc non abusive, de toute *D.C.P.*
- *Illustration(s) :*
  Pour effectuer le traitement de remboursement de frais de santé, il n'est pas nécessaire d'avoir collecté et stocké toutes autres catégories de *D.C.P.*, autres que celles nécessaires à ce traitement (*à savoir :* NIR ou n° adhérent mutuelle, nom, prénom, code prise en charge, etc.).

❑ ***Principe spécifique de « exactitude des données » :***

- *Intitulé :*
  « …exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude) ; »
- *Explication :*
  Les licéité et loyauté d'un traitement, sinon toute forme de consentement à l'utilisation de *D.C.P.*, ne vaut que pour effectuer des traitements corrects, sur des données correctes
- *Justification(s) :*
  Un traitement (même correct) de *D.C.P.* incorrecte (inexacte ou incomplète) risque d'engendrer une perte de chance pour la *Personne Concernée*
- *Illustration(s) :*
  Si une *Personne Concernée* peut bénéficier d'un droit légitime (aide sociale ou allocation…) à partir de… tel âge ; et que son âge (ou sa date de naissance) est erronée dans les bases du *Responsable du Traitement*, alors il risque de s'en suivre une non-attribution de cette aide / allocation, pourtant légitime

SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]

La Protection des Données à caractère Personnelles [P.D.P.]

Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers

TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

❑ ***Principes spécifiques de « confidentialité & intégrité [des données] »***

❖ *Intitulé :*

« …traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) ; »

❖ *Explication :*

Ce double principe (confidentialité & intégrité) est étroitement lié aux principes suivants : *"exactitude"*, *"limitation des finalités"*, *"minimisation des données"*

❖ *Justification(s) :*

La sécurité des données (du Système d'Information, d'une manière générale) ne peut que contribuer, très significativement, à la protection des *D.C.P.*

❖ *Illustration(s) :*

Des mesures de sécurité organisationnelles (i.e., contrôle des accès logiques) et techniques (i.e., chiffrer les *D.C.P.* stockées, contrôler l'intégrité de la base) contribuent (ensemble), à respecter (conjointement), les exigences relatives à la confidentialité de ces *D.C.P.* et celles relatives à l'intégrité de ces *D.C.P.*

SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]

La Protection des Données à caractère Personnelles [P.D.P.]

*Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers

TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

SENSIBILISATION AUX ENJEUX DE P… …S D.C.P.

Genèse & Historique / Principes génériques & …de base / Acteurs & R… ***…esponsabilités***

Pour mémoire : les 8 droits des personnes

Droits légitimes de la Personne Concernée [P.C.]

1. ***Droit à être informé*** *(ex-obligation d'information)* *[articles #13 & #14]*
2. ***Droit d'accès à ses données par la Personne Concernée*** *[article #15]*
3. ***Droit de rectification*** *(… des données inexactes)* *[article #16]*
4. ***Droit à l'effacement*** *[dit « droit à l'oubli »]* *[article #17]*
5. ***Droit à la limitation du traitement*** *[article #18]*
6. ***Obligation de notification*** *(…des rectification/effacement)* *[article #19]*
7. ***Droit à la portabilité des données*** *(… vers un autre R.T.)* *[article #20]*
8. ***Droit d'opposition*** *(…à tout moment, …fins de prospection)* *[article #21]*

➔ **Autant de *responsabilités* incombant au responsable du traitement**
(…et preuve de sa responsabilité : obligation constante de ***"accountability"***)

❑ ***Le « droit à la transparence (droit d'information) »***

- ❖ *Explication :*
  La *Personne Concernée* a droit d'avoir connaissance des toutes les utilisations qui sont faites de ses *D.C.P.* qui sont confiées au *Responsable du Traitement*
- ❖ *Illustration(s) :*
  Lors de la collecte de *D.C.P.* auprès d'un nouvel adhérent, une mutuelle doit lui préciser quels sont, exactement, les traitements (finalités) qui sont réalisés

❑ ***Le « droit d'accès »***

- ❖ *Explication :*
  Ce droit est l'application des principes de licéité / de loyauté / de transparence
- ❖ *Justification(s) :*
  Il correspond également à l'exercice par la *P.C.* de son *"droit à la transparence"*

❑ ***La notion de « consentement »***

- ❖ *Explication :*
  Sans autre motif légitime, le R.T. doit obtenir le consentement de la *P.C.*
- ❖ *Justification(s) :*
  Sans la moindre ***licéité implicite***, le *R.T.* doit recueillir une ***licéité explicite***

SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]
La Protection des Données à caractère Personnelles [P.D.P.]
Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers
TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

❑ ***Le « droit de rectification »***

- ❖ *Explication :*
  En application des principes *"exactitude"* et *"intégrité"*, la *Personne Concernée* peut exiger du *R.T.* de faire rectifier ses *D.C.P.* erronées et/ou incomplètes
- ❖ *Illustration(s) :*
  Un adhérent d'une mutuelle peut faire rectifier une donnée erronée relative à la composition du foyer, afin de bénéficier de la couverture à laquelle elle a droit

❑ ***Le « droit à l'effacement (droit à l'oubli) »***

- ❖ *Explication :*
  La *Personne Concernée* pouvant retirer son consentement à tout moment, et s'il n'y a pas d'autre motif légitime pour maintenir le traitement de ses *D.C.P.*, alors la *Personne Concernée* peut exiger que ses *D.C.P.* ne figurent plus dans les traitements considérés, sinon de façon pseudonymisée (voire anonymisée)
- ❖ *Justification(s) :*
  La préservation de l'intimité et donc la protection des droits et libertés de toute *Personne Concernée* impose de ne plus pouvoir traiter des *D.C.P.* sans licéité
- ❖ *Illustration(s) :*
  Retrait de tout ex-adhérent, de la *Mailing List* d'une *newsletter* d'une mutuelle

❑ ***Le « droit à la limitation du traitement »***

- *Explication :*
  En application des principes de *« licéité / loyauté / transparence"* et *« limitation des finalités [du traitement]"*, la *Personne Concernée* peut exiger du *R.T.* de limiter ses traitements (du *R.T.*) de ses *D.C.P.* (de la *P.C.*), aux strictes *D.C.P.* nécessaires, ainsi qu'aux strictes finalités de traitement qui sont légitimes
- *Illustration(s) :*
  Un adhérent d'une mutuelle peut exiger du *R.T.* de n'utiliser ses coordonnées postales pour, et uniquement pour, la finalité légitime (adresser les décomptes)

❑ ***Le « droit d'opposition »***

- *Intitulé :*
  « La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant […] y compris un profilage […]. »
- *Justification(s) :*
  Ce droit est lié à la possibilité, pour la *P.C.* (selon sa situation), de retirer à tout moment son consentement et, ainsi, de s'opposer au traitement considéré

SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]
La Protection des Données à caractère Personnelles [P.D.P.]
Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers
TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

❑ ***Le « droit à la portabilité des données »***

- *Intitulé :*
  « Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle, […]. [Art. 20] »
- *Explication :*
  Ce droit permet de ne pas rester dépendant d'un *R.T.* pour de simples raisons uniquement technologiques (format / structure des *D.C.P.* confiées au *R.T.*)
- *Justification(s) :*
  Ce droit contribue directement à préserver les droits et libertés fondamentales des *P.C.*, en leur permettant de choisir leur *R.T.* en fonction de critère objectifs
- *Illustration(s) :*
  Une *P.C.* résilie son adhésion à la *Mutuelle-X* (couverture-santé inappropriée) pour adhérer à la *Mutuelle-Y* (couverture-santé nettement plus appropriée), en portant ses *D.C.P.*, depuis le *R.T.* de la *Mutuelle-Y* vers le *R.T.* de la *Mutuelle-Y*

SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]

La Protection des Données à caractère Personnelles [P.D.P.]

Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers

TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

❑ ***Les « obligations du Responsable du Traitement [R.T.] »***

❖ *Explication :*

Le *R.T.* est redevable envers toute *P.C.* d'assumer ses responsabilités de *R.T.* exigibles à travers le *R.G.P.D.* :

✓ et notamment, d'appliquer les *2 principes génériques du R.G.P.D.* :
Protection-par-Défaut & ***Protection-dès-la-Conception***

✓ ainsi que les *10 principes spécifiques du R.G.P.D.*:
Licéité-Loyauté-Transparence, ***Minimisation***, ***Limitations (finalités, durées)***, ***Exactitude***, ***Confidentialité & Intégrité*** et… sa ***Responsabilité***

…afin d'être en mesure de respecter les libertés et droits fondamentaux des *P.C.* en permettant à toute *P.C.* d'exercer :

✓ ses *8 droits spécifiques du R.G.P.D.*:
Information, ***Accès***, ***Rectification***, ***Opposition***, ***Effacement***, ***Portabilité***, ***Refus de toute décision exclusivement automatisée***, ***Limitation du traitement***

❖ *Justification(s) :*

C'est au *R.T.* d'assumer ses responsabilités… en tant que *R.T.* ; ainsi, c'est au *R.T.* (ou bien à son *DPD/DPO*) qu'une *P.C.* doit s'adresser pour exercer ses *8* droits spécifiques

❖ *Illustration(s) :*

Plutôt que de devoir s'adresser au service informatique de sa mutuelle ou à l'hébergeur en infogérence de cette mutuelle (i.e., son fournisseur d'hébergement pour ses *D.C.P.*), la *P.C.* s'adresse directement à sa mutuelle pour exercer ses *8* droits spécifiques

SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]

La Protection des Données à caractère Personnelles [P.D.P.]

Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers

TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

❑ ***Notions de « profilage » et « décision exclusivement automatisée »***

❖ *Intitulé :*

« toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique. [Art. 4] »

❖ *Explication :*

Cette notion est à rapprocher des principes de *"loyauté"* et de *"transparence"*

❖ *Justification(s) :*

Toute *Personne Concernée* a la droit de s'opposer à toute décision *« …fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative… »*

❖ *Illustration(s) :*

Une mutuelle ne peut refuser de prendre en charge un nouvel adhérent à la suite d'une décision motivée par un seul traitement exclusivement automatisé

SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]

La Protection des Données à caractère Personnelles [P.D.P.]

Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers

TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

❑ ***Notions de « pseudonymisation » et « anonymisation »***

❖ *Intitulé :*

*« Le traitement de données à caractère personnel de telle façon que celles-ci **ne puissent plus être attribuées à une personne concernée précise** sans avoir **recours à des informations supplémentaires**, pour autant que ces informations supplémentaires soient **conservées séparément** et soumises à des **mesures techniques et organisationnelles** afin de garantir que les données à caractère personnel ne sont **pas attribuées à une personne physique identifiée ou identifiable**. [Art. 4] »*

❖ *Explication :*

Ces notions sont à rapprocher des principes de limitations (données & durées)

❖ *Justification(s) :*

Toute *Personne Concernée* a droit à l'*anonymisation*, sinon *pseudonymisation*, de ces *D.C.P.*, si le traitement concerné n'est plus licite, ni même légitime

❖ *Illustration(s) :*

Une mutuelle peut continuer à effectuer un traitement statistique individualisé, y compris sur un ex-adhérent (afin de ne pas biaiser les statistiques), pourvu que ce-dernier ne puisse pas être ré-identifié (pas d'appariement nominatif)

SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]

La Protection des Données à caractère Personnelles [P.D.P.]

Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers

TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

❑ ***Notions de « données génétiques » et « données biométriques »***

❖ *Intitulés :*

*"données génétiques" : les données à caractère personnel relatives aux **caractéristiques génétiques héréditaires ou acquises** d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question. [Art. 4] »*

*"données biométriques" : les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux **caractéristiques physiques**, **physiologiques** ou **comportementales** d'une **personne physique**, qui **permettent ou confirment son identification unique**, telles que des images faciales ou des données dactyloscopiques. [Art. 4] »*

❖ *Justification(s) :*

Ces deux catégories de *D.C.P.* sont les plus immuables et, par conséquent, les plus risquées envers la protection de l'intimité des *Personnes Concernée* et, donc, les plus dangereuses vis-à-vis du respect de ses droits et ses libertés

❖ *Illustration(s) :*

Exploitation de données biométriques dans un dispositif d'authentification forte

❑ *Notions de « violation de données personnelles »*

- ❖ *Intitulé :*
  "violation de données à caractère personnel" : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données »
- ❖ *Explication :*
  Cette notion est à rapprocher des principes de limitation (données & durée
- ❖ *Justification(s) :*
  Toute *Personne Concernée* a le droit à l'anonymat (ou au pseudonymat), lorsque les traitements concernés ne sont plus licites, ni légitimes
- ❖ *Illustration(s) :*
  Une mutuelle peut continuer à effectuer un traitement statistique individualisé, y compris sur un ex-adhérent (afin de ne pas biaiser les statistiques), pourvu que ce-dernier ne puisse pas être re-identifier (pas d'appariement nominatif)

SENSIBILISATION AUX ENJEUX DE LA PROTECTION DES D.C.P.

*Genèse & Historique / **Principes g**énériques de mise base / **Acteurs & Responsabilités***

En guise d'exercice d'application

Afin de vérifier l'adéquation des *principes de base exigibles* au titre du *R.G.P.D.*
[et qui reposent sur la… (preuve de…) responsabilité du Responsable du Traitement]
avec les différents *droits qui peuvent être exercés* par toute personne concernée, voici un exercice qui permet de rapprocher *ces 6-à-9 principes* avec *ces 8+3 droits* :

Licéité, loyauté et transparence ❑	❑ *Droit à être informé* [art. #13 #14]
	❑ *Droit d'accès* [art. #15]
Limitation des finalités ❑	❑ *Droit de rectification* [art. #16]
Minimisation des données ❑	❑ *Droit à l'effacement ("oubli")* [art. #17]
	❑ *Droit à la limitation du trait.t* [art. #18]
Exactitude des données ❑	❑ *Droit à la portabilité* [art. #20]
Limitation de la conservation ❑	❑ *Droit d'opposition* [art. #21]
	❑ *Droit de "refuser" le profilage* [art. #22]
Intégrité et confidentialité ❑	❑ *Obligation d'être notifié [r+e+l]* [art. #19]

SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]

La Protection des Données à caractère Personnelles [P.D.P.]

Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers

TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

SENSIBILISATION AUX ENJEUX DE LA PROTECTION DES D.C.P.

*Genèse & Historique / Principes génériques & …de base / **Acteurs & Responsabilités***

Les "vrais" enjeux actuels du R.G.P.D.

1. ***Enjeux de mise-en-conformité** (vis-à-vis des obligations du R.G.P.D.)*
2. ***Enjeux de maintien-en-conformité** (aux obligations du R.G.P.D.)*
3. ***Enjeux juridiques pour les entreprises** (privées)*
4. ***Enjeux juridiques pour les administrations** (publiques)*
5. ***Enjeux financiers** (coûts de la mise en conformité, etc.)*
6. ***Enjeux financiers** (risques en cas de non-conformité, etc.)*
7. ***Enjeux d'image interne** (cf. R.H.), **image externe** (clients/usagers)*
8. ***Enjeux liés à la réputation** (relation[s] avec la CNIL, les partenaires)*
9. ***Enjeux de Protection des Données Personnelles** (en lien direct avec le R.G.P.D.)*
10. ***Enjeux de Sécurité du Système d'Information** (de manière générale)*

À titres purement illustratifs

SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]

La Protection des Données à caractère Personnelles [P.D.P.]

Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers

TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

SENSIBILISATION AUX ENJEUX DE LA PROTECTION DES D.C.P.

*Genèse & Historique / Principes génériques & …de base / **Acteurs & Responsabilités***

Les "pistes" de la conformité au R.G.P.D.

- ***Mise en conformité au R.G.P.D.*** → cartographies des données / traitements / flux / etc.
- ***Coût de la mise en conformité*** → projet interne et/ou accompagnement(s) externe(s)
- ***Maintien de la conformité au R.G.P. D.*** → mise à jour régulière des cartographie / etc.
- ***Coût du maintien en conformité*** → …désignation d'un D.P.D. (interne, externe, mutualisé)
- ***Risque de sanction financière en cas de manquement*** → 2% à 4% C.A. ou 10 à 20 M€
- ***Risque de sanctions pénales*** (cf. Loi Informatique et Libertés : LIL1, LIL2, LIL3)
- ***Image de marque et confiance du point de vu du personnel*** (cf. traitements RH)
- ***Image de marque et confiance du point de vue des partenaires*** (cf. fournisseurs)
- ***Mise en place des mesures organisationnelles/techniques de sécurité*** (conformité !)
- ***Mise en place de démarches/solutions/outils de gestion des incidents*** (accidentels ?)
- ***Mise en place de démarches/solutions/outils de gestion des violations*** (intentionnelles ?)
- ***Mise en place de démarches/solutions/outils de management du risque*** (informatique ?)
- ***Mise en place de démarches/solutions/outils de management qualité*** (de l'information ?)

Un savant mélange entre *S.S.I.* et *P.D.P.*

❑ *Prise en compte, par défaut, du cycle de vie de la donnée*

Culture générale en informatique

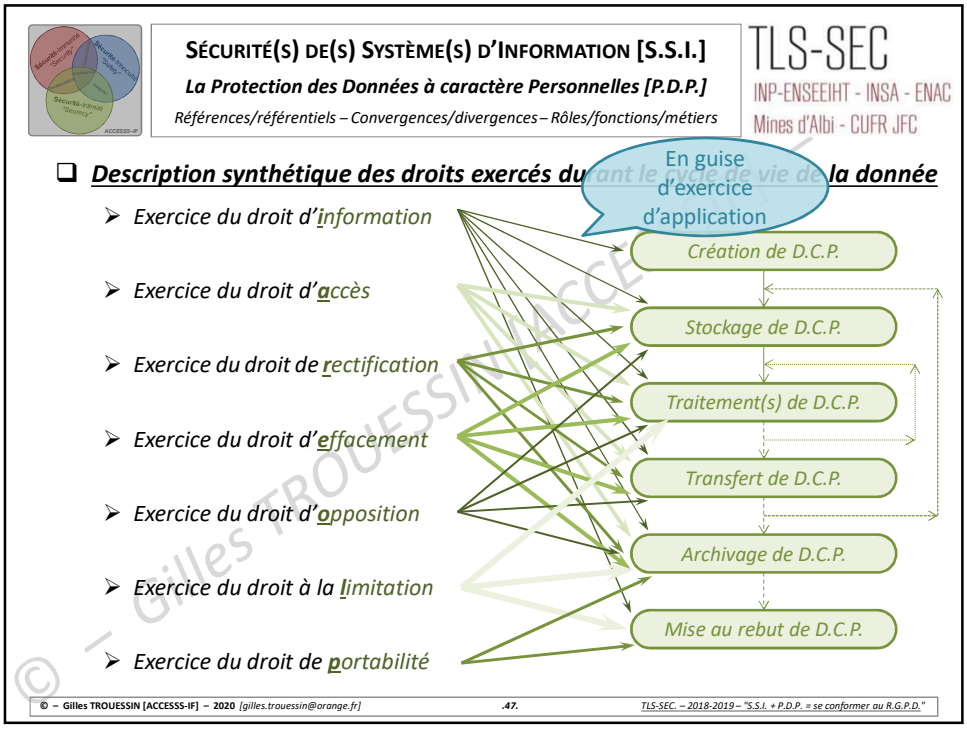
- *Pour la phase de **création** (collecte directe / indirecte)*
  - *Obligation d'information par responsables de traitement lors de la collecte directe*
  - *Obligation d'information sur exercice du droit d'information par la P.C.*
- *Pour la phase de **stockage** (fiabilisé et sécurisé)*
  - *IDEM : obligation de respecter l'exercice de divers droits de la Personne Concernée*
- *Pour la phase de **traitement** (autorisé et sécurisé)*
  - *IDEM : obligation de respecter l'exercice de divers droits de la Personne Concernée*
- *Pour la phase de **transfert** (autorisé et sécurisé)*
  - *IDEM : obligation de respecter l'exercice de divers droits de la Personne Concernée*
- *Pour la phase de d'**archivage** (fiabilisé et contrôlé)*
  - *IDEM : obligation de respecter l'exercice de divers droits de la Personne Concernée*
- *Pour la phase de **mise au rebus** (suppression ou purge)*
  - *IDEM : obligation de respecter l'exercice de divers droits de la Personne Concernée*

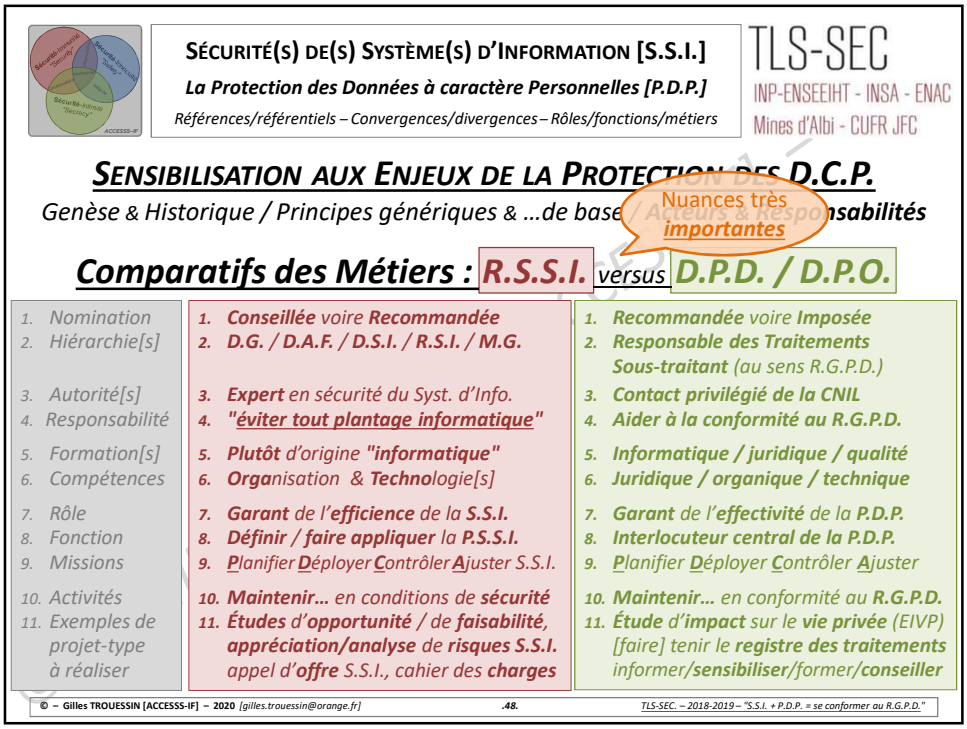
SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]
La Protection des Données à caractère Personnelles [P.D.P.]
Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers
TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

❑ *Prise en compte , dès la conception, des droits sur la donnée*

Culture générale issue du ***R.G.P.D.***

- *Pour l'exercice du droit d'**i**nformation*
  - *À tout moment sur demande d'exercice de ce droit par la Personne Concernée*
- *Pour l'exercice du droit d'**a**ccès*
  - *À tout moment sur demande d'exercice de ce droit par la Personne Concernée*
- *Pour l'exercice du droit à la **p**ortabilité*
  - *Si la Personne Concernée décide de changer de responsable de traitement*
- *Pour l'exercice du droit d'**e**ffacement*
  - *Si la Personne Concernée décide d'exercer son droit « à l'oubli »*
- *Pour l'exercice du droit d'**o**pposition*
  - *Par exemple : lors que la Personne Concernée décide de retirer son consentement*
- *Pour l'exercice du droit de **r**ectification*
  - *Si la Personne Concernée constate une imprécision et/ou une omission*


SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]
La Protection des Données à caractère Personnelles [P.D.P.]
Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers
TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC
Description synthétique des droits exercés durant le cycle de vie de la donnée
Exercice du droit d'information
Exercice du droit d'accès
Exercice du droit de rectification
Exercice du droit d'effacement
Exercice du droit d'opposition
Exercice du droit à la limitation
Exercice du droit de portabilité
En guise d'exercice d'application
Création de D.C.P.
Stockage de D.C.P.
Traitement(s) de D.C.P.
Transfert de D.C.P.
Archivage de D.C.P.
Mise au rebut de D.C.P.
© – Gilles TROUESSIN [ACCESSS-IF] – 2020 [gilles.trouessin@orange.fr] .47. TLS-SEC. – 2018-2019 – "S.S.I. + P.D.P. = se conformer au R.G.P.D."


SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]
La Protection des Données à caractère Personnelles [P.D.P.]
Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers
TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC
SENSIBILISATION AUX ENJEUX DE LA PROTECTION DES D.C.P.
Genèse & Historique / Principes génériques & …de base / Acteurs & Responsabilités
Nuances très importantes
Comparatifs des Métiers : R.S.S.I. versus D.P.D. / D.P.O.
1. Nomination
2. Hiérarchie[s]
3. Autorité[s]
4. Responsabilité
5. Formation[s]
6. Compétences
7. Rôle
8. Fonction
9. Missions
10. Activités
11. Exemples de projet-type à réaliser
1. Conseillée voire Recommandée
2. D.G. / D.A.F. / D.S.I. / R.S.I. / M.G.
3. Expert en sécurité du Syst. d'Info.
4. "éviter tout plantage informatique"
5. Plutôt d'origine "informatique"
6. Organisation & Technologie[s]
7. Garant de l'efficience de la S.S.I.
8. Définir / faire appliquer la P.S.S.I.
9. Planifier Déployer Contrôler Ajuster S.S.I.
10. Maintenir… en conditions de sécurité
11. Études d'opportunité / de faisabilité, appréciation/analyse de risques S.S.I. appel d'offre S.S.I., cahier des charges
1. Recommandée voire Imposée
2. Responsable des Traitements Sous-traitant (au sens R.G.P.D.)
3. Contact privilégié de la CNIL
4. Aider à la conformité au R.G.P.D.
5. Informatique / juridique / qualité
6. Juridique / organique / technique
7. Garant de l'effectivité de la P.D.P.
8. Interlocuteur central de la P.D.P.
9. Planifier Déployer Contrôler Ajuster
10. Maintenir… en conformité au R.G.P.D.
11. Étude d'impact sur le vie privée (EIVP) [faire] tenir le registre des traitements informer/sensibiliser/former/conseiller
© – Gilles TROUESSIN [ACCESSS-IF] – 2020 [gilles.trouessin@orange.fr] .48. TLS-SEC. – 2018-2019 – "S.S.I. + P.D.P. = se conformer au R.G.P.D."

SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]

La Protection des Données à caractère Personnelles [P.D.P.]

Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers

TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

SENSIBILISATION AUX ENJEUX DE LA PROTECTION DES D.C.P.

*Genèse & Historique / Principes génériques & …de base / **Acteurs** & Responsabilités*

Nuances très ***importantes***

Convergences / Divergences entre : la S.S.I. et la P.D.P.

	S.S.I.	P.D.P.
✓ *Principales convergences*	✓ ***Une activité centrale, autour du R.S.S.I.***	✓ ***Une activité centrale, gérée par le D.P.O.***
	✓ ***Référentiel des bonnes pratiques :*** *avec la série des normes **ISO-IEC 27xxx***	✓ ***Référentiel de pratiques exigées*** *par le **R.G.P.D.** (173 considérants / 65 articles)*
	✓ ***Démarches ponctuelles d'audits** en SSI, **analyses de risques**-SSI et **projets**-SSI*	✓ ***Démarches ponctuelles d'audits**-PDP, **analyses d'impacts (EIVP, DPIA)**, etc.*
	✓ ***Démarche itérative possible**, de type : Planifier–Déployer–Contrôler–Ajuster*	✓ ***Démarche itérative possible**, de type : Planifier–Déployer–Contrôler–Ajuster*
✓ *Principales divergences*	✓ ***Pas d'obligation intrinsèque de S.S.I.*** *(i.e., juridique = légal + réglementaire)*	✓ ***Obligation intrinsèque de P.D.P.*** *de par les sanctions **pénales** et/ou **financières***
	✓ ***Exigences extrinsèques de S.S.I.*** *issues d'accords **contractuels/clients**, etc.*	✓ ***Exigences extrinsèques de P.D.P.*** *de par le respect des **personnes concernées***
	✓ ***Prioritairement :*** *sous influences des **directions-économiques (D.A.F., D.A.J.)***	✓ ***Prioritairement :*** *le D.P.O. ne doit pas exercer sous une quelconque influence*
	✓ ***Secondairement :*** *être aux services des utilisateurs (directions-métier -internes)*	✓ ***Prioritairement :*** *la P.D.P. doit servir les individus (licéité-loyauté-transparence)*

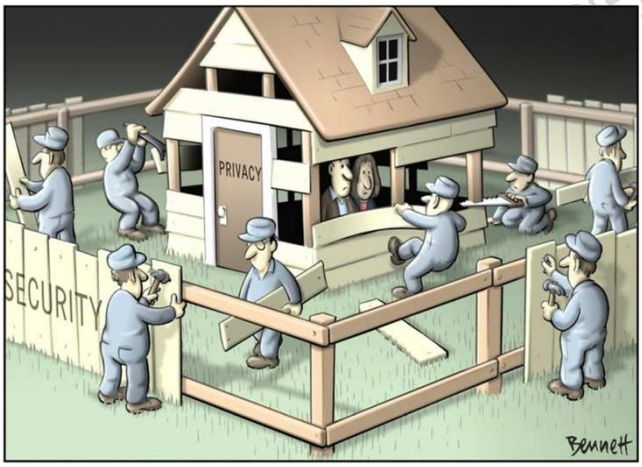
SÉCURITÉ(S) DE(S) SYSTÈME(S) D'INFORMATION [S.S.I.]

La Protection des Données à caractère Personnelles [P.D.P.]

Références/référentiels – Convergences/divergences – Rôles/fonctions/métiers

TLS-SEC
INP-ENSEEIHT - INSA - ENAC
Mines d'Albi - CUFR JFC

Conclusion centrale : "qui de la S-Immunité / S-Intimité est au service de l'autre ?"



Je vous remercie pour votre attention : avez-vous des questions !?