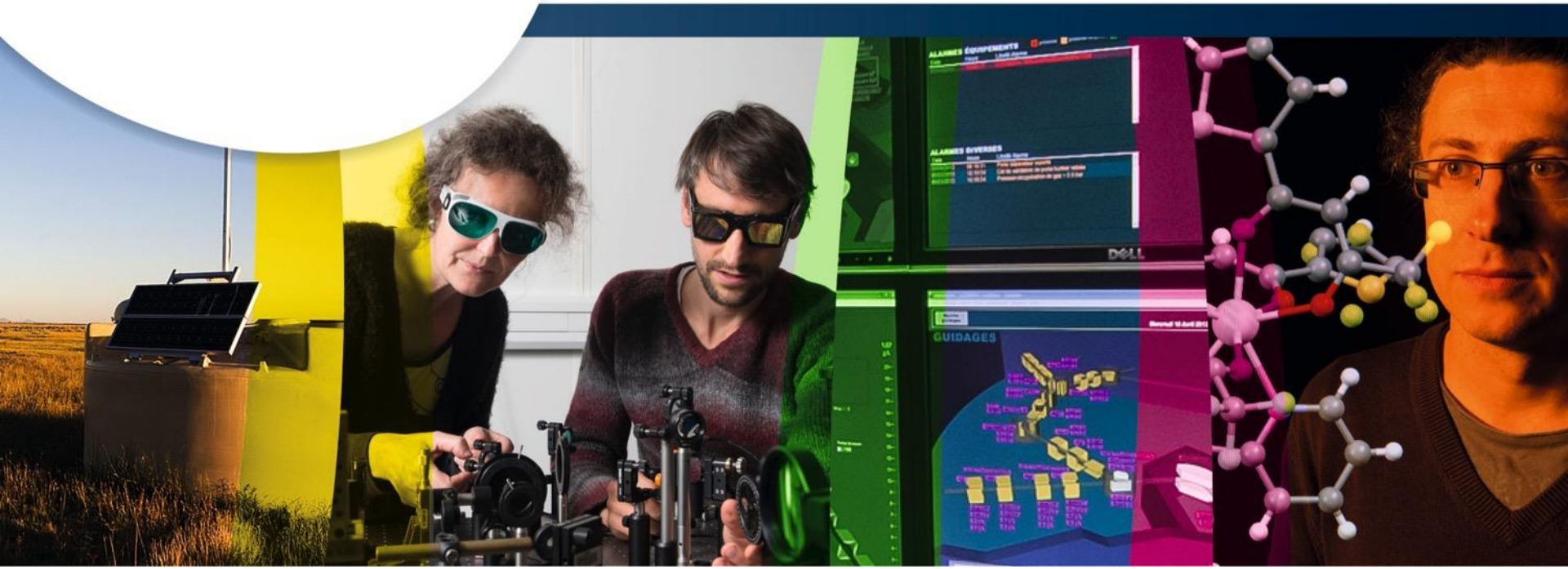
www.cnrs.fr

Législation réglementation



www.cnrs.fr

Réglementation sur les données à caractère personnel

De la loi informatique et libertés au RGPD

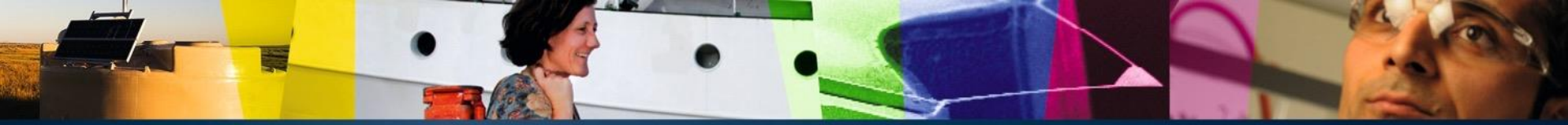
www.cnrs.fr

- Loi informatiques et libertés
  - 1978
  - Modifiée depuis
- Règlement européen sur la protection des données (RGPD)
  - Applicable au 25 mai 2018
- Inversion des paradigmes
  - En France on est conforme ou non à la loi
- Avec le RGPD il faut conserver la preuve que l'on a mis en œuvre des mécanismes et procédures internes pour s'y conformer
  - ***Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui- ci est respecté*** (responsabilité). (Art. 5)

Données à caractère personnel

www.cnrs.fr

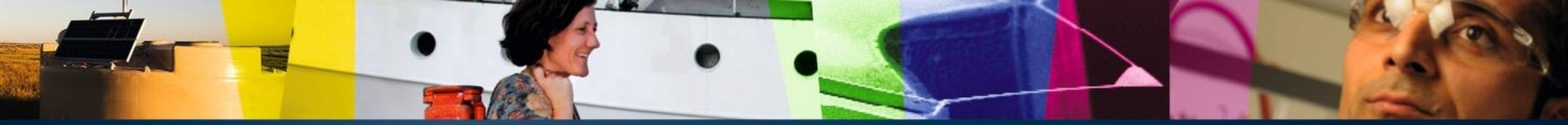
- Concernent les personnes physiques
  - Identifiées directement : nom par exemple
  - Identifiables indirectement : permet de retrouver la personne
    - N° d'immatriculation
    - N° de téléphone
    - Photographie
    - Éléments biométriques
    - Adresse IP
    - Date de naissance + commune de résidence
    - Etc.
- Question à se poser
  - Est-ce que le recoupement des informations permet de déterminer avec une forte probabilité quel est l'individu ?



Principes

www.cnrs.fr

- Finalité
  - Usage légitime correspondant aux missions de l'organisme
- Proportionnalité
  - Seulement les informations nécessaires et pertinentes
- Durée de conservation limitée
  - En accord avec la finalité
- Sécurité et confidentialité
  - Le responsable du traitement est astreint à une obligation de sécurité
- Transparence
  - Information des personnes, droit d'accès



Analyse d'impact relative à la protection des données (PIA)

www.cnrs.fr

- *Lorsqu'un type de traitement, en particulier par le recours aux nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un **risque élevé pour les droits et les libertés des personnes physiques,** les États membres prévoient que le responsable du traitement effectue préalablement au traitement une **analyse de l'impact des opérations** de traitement envisagées sur la protection des données à caractère personnel.*
- *L'analyse visée au paragraphe 1 contient au moins une description générale des opérations de traitement envisagées, une évaluation des risques pour les droits et libertés des personnes concernées, les mesures envisagées pour faire face à ces risques, les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à **apporter la preuve du respect de la présente directive**, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes touchées.* (Art. 27)

Comment conduire un PIA ?

www.cnrs.fr

- Méthode de la CNIL
- A mener de pair avec l'analyse des risques du système d'information
  - PIA
    - Impacts pour les personnes
  - Analyse des risques du SI
    - Impacts sur l'organisme
  - Impacts sur les personnes ➔ impacts sur l'organisme
    - Image
    - Juridique
    - Coûts pour prévenir les personnes

Security/privacy by design/default

- Loi informatique et libertés
  - Obligation de protection
- RGPD
  - *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****.(Art. 78)*

Du CIL au DPO

www.cnrs.fr

- Loi informatique et libertés → correspondant informatique et libertés (CIL)
  - Tient un registre des traitements soumis à déclaration
  - Transmets les demandes d'autorisation
- RGPD → délégué à la protection des données
  - Garant du respect du RGPD
    - Plus de déclaration obligatoire mais on doit conserver les preuves de la sécurité
  - Déclaration sans délai des incidents et information des personnes concernées
    - Nouveauté du RGPD
- Systématiquement contacter le service du CIL
  - En amont de tout projet traitant de données à caractère personnel
  - En cas d'incident

Que doit faire un développeur ?

www.cnrs.fr

- Devoir de conseil et d'alerte du responsable de traitement, du donneur d'ordres
- S'assurer que le CIL a été contacté en amont du projet
- S'assurer de l'existence d'une analyse de risques (PIA) et la prendre en compte
- Security/privacy by design/default
- Principe d'économie : n'avoir que les informations nécessaires
- Anonymisation, pseudonymisation
- Chiffrement
- Documentation → preuve
- Déclarer les incidents dont il aurait pu avoir connaissance

www.cnrs.fr

Des atteintes aux systèmes de traitement automatisé de données

Système de traitement automatisé de données

www.cnrs.fr

- STAD → expression utilisée dans la loi
  - Tout système de traitement de l'information : de l'objet connecté au supercalculateur en passant par un disque dur
  - Jurisprudence très extensive
- Articles 323-1 et suivants du code pénal répriment
  - Accéder ou se maintenir, frauduleusement
  - Entraver ou fausser le fonctionnement
  - Introduire frauduleusement des données
  - Extraire, détenir, reproduire, transmettre, supprimer ou modifier frauduleusement des données
  - Jusqu'à 10 ans d'emprisonnement et 300 000€ d'amende

Test d'intrusion

www.cnrs.fr

- Article 323-3-1
  - *Le fait, **sans motif légitime**, notamment de recherche ou de **sécurité informatique**, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.*
- Se fait dans le cadre d'une exception
- Nécessité absolue d'un accord de toutes les parties concernées (y compris réseau de transit)
- On ne teste que son propre système ou ceux pour lesquels une demande expresse a été formulée
- Publication par l'ANSSI d'un référentiel d'exigences applicable aux prestataires d'audit de la sécurité des systèmes d'information (PASSI)
- **Les outils d'attaques que nous allons vous montrer reste dans ce cadre**

Que doit faire un développeur ?

www.cnrs.fr

- Détenir et utiliser les seuls outils de recherche de failles qui sont nécessaires à l'analyse de ses développements
- Protéger ces outils afin qu'ils ne soient pas utilisés à son insu
- Ne jamais chercher à attaquer autrui
- La recherche de failles (puis leur correction) fait partie des bonnes pratiques de développement

www.cnrs.fr

Politique de sécurité des systèmes d'information de l'État (PSSIE)

Sécurité du développement des systèmes

www.cnrs.fr

- Tous nos SI sont concernés par la PSSIE
- *Objectif 29 : reconnaître la sécurité comme une fonction essentielle, et la prendre en compte dès la conception des projets.*
  - *DEV-INTEGR-SECLOC : intégrer la sécurité dans les développements locaux. Toute initiative locale de développement informatique doit respecter les exigences nationales en matière de SSI, concernant la prise en compte de la sécurité dans les projets et les développements informatiques. Le service à l'origine du projet se porte garant de l'application du référentiel général de sécurité, et de l'application d'une démarche d'homologation du système.*

Sécurité du développement des systèmes

www.cnrs.fr

- *Objectif 29 : reconnaître la sécurité comme une fonction essentielle, et la prendre en compte dès la conception des projets.*
  - *DEV-SOUS-TRAIT : intégrer des clauses SSI dans les contrats de sous-traitance de développement informatique. Lors de l'écriture d'un contrat de sous-traitance de développement, plusieurs clauses relatives à la SSI doivent être intégrées :*
    - *formation obligatoire des développeurs sur le développement sécurisé et sur les vulnérabilités classiques ;*
    - *utilisation obligatoire d'outils permettant de minimiser les erreurs introduites durant le développement (outils gratuits d'analyse statique de code, utilisation de bibliothèques réputées pour leur sécurité, etc.) ;*
    - *production de documentation technique décrivant l'implantation des protections développées (gestion de l'authentification, stockage des mots de passe, gestion des droits, chiffrement, etc.) ;*
    - *respect de normes de développement sécurisé, qu'elles soient propres au développeur, publiques ou propres au commanditaire ;*
    - *obligation pour le prestataire de corriger, dans un temps raisonnable et pour un prix défini, les vulnérabilités introduites durant le développement et qui lui sont remontées, en incluant automatiquement les corrections des autres occurrences des mêmes erreurs de programmation.*

Sécurité du développement des systèmes

www.cnrs.fr

- *Objectif 30 : mener les développements logiciels selon une méthodologie de sécurisation du code produit.*
  - *DEV-FUITES : limiter les fuites d'information.*
  - *DEV-LOG-ADHER : réduire l'adhérence des applications à des produits ou technologies spécifiques*
  - *DEV-LOG-CRIT : instaurer des critères de développement sécurisé*
  - *DEV-LOG-CYCLE : intégrer la sécurité dans le cycle de vie logiciel*
  - ***DEV-LOG-WEB : améliorer la prise en compte de la sécurité dans les développements Web***
  - *DEV-LOG-PASS : calculer les empreintes de mots de passe de manière sécurisée*

Sécurité du développement des systèmes

www.cnrs.fr

- *Objectif 31 : accompagner le développement sécurisé d'applications à risques par des contre-mesures minimisant l'impact d'attaques nouvelles.*
  - *DEV-FILT-APPL : mettre en œuvre des fonctionnalités de filtrage applicatif pour les applications à risque. Devant les applications à risques, il est recommandé de faire usage d'une solution tierce de filtrage applicatif.*

Que doit faire un développeur ?

www.cnrs.fr

- Prendre en compte la sécurité dès le démarrage du projet et tout au long de son cycle de développement
- Mettre en œuvre les bonnes pratiques de développement

Politique de sécurité de l'information du CNRS

www.cnrs.fr

Développement des SI

www.cnrs.fr

- *DEV-1*
  - *Tout projet informatique/scientifique doit respecter les exigences nationales en matière de sécurité des Systèmes d'Information et prendre en compte la sécurité dès son démarrage.*

www.cnrs.fr

Référentiel général de sécurité (RGS)

Obligations du RGS

www.cnrs.fr

- Domaine d'application
  - Téléservices, services aux usagers ou entre administrations
- Prendre en compte la SSI dans les projets
- Règles
  - Mécanismes d'authentification
  - Gestion de la confiance (certificats)
  - Utilisation de la cryptographie
    - Algorithmes
    - Tailles de clés

Que doit faire un développeur ?

www.cnrs.fr

- Intégrer la SSI dans le projet
- Se conformer au RGS (annexes) pour le choix
  - Algorithmes
  - Tailles de clés
  - Mode de chiffrement
- En pratique mettre en œuvre les recommandations du guide de l'ANSSI *Recommandations de sécurité relatives à TLS*

www.cnrs.fr

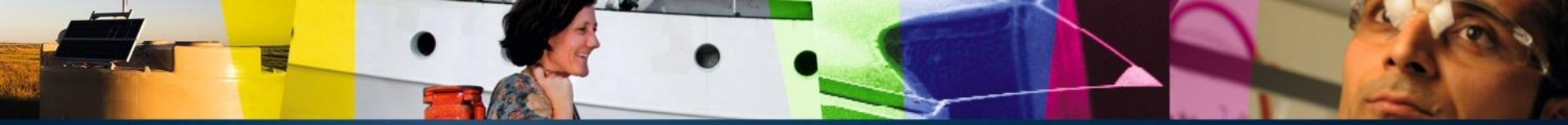
Référentiel général d'interopérabilité (RGI)

RGI

- Le RGI est un cadre de recommandations référençant des normes et standards qui favorisent l'interopérabilité au sein des systèmes d'information de l'administration.
- La version 2.0 du RGI est officialisée par l'arrêté en date du 20 avril 2016
  - http://references.modernisation.gouv.fr/interoperabilite

www.cnrs.fr

Référentiel général d'accessibilité des administrations (RGAA)



RGAA

www.cnrs.fr

- Les informations diffusées doivent être accessibles à tous y compris aux personnes en situation de handicap
- La version 3.0 du RGAA a été approuvée par l'arrêté du 29 avril 2015
  - http://references.modernisation.gouv.fr/rgaa-accessibilite/

www.cnrs.fr

Protection du potentiel scientifique et technique (PPST)

PPST

www.cnrs.fr

- Cadre juridique
  - Articles 413-7 (partie législative) et R413-5-1 (partie réglementaire) du code pénal
  - Décret n° 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation
  - Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation
  - Circulaire du novembre 2012
  - Notes thématiques du ministère

PPST

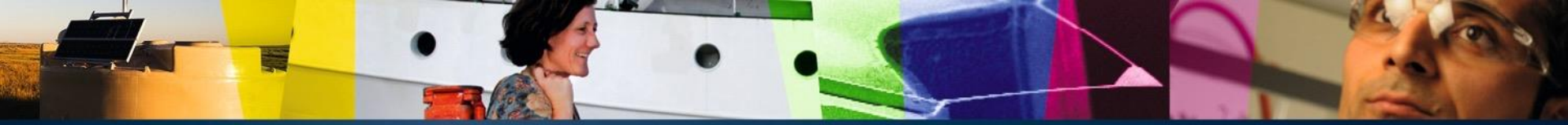
www.cnrs.fr

- Potentiel scientifique et technique
  - Extension de ce qui concerne la défense nationale
  - Introduit une qualification pénale pour des faits qu'il était difficile de réprimer auparavant
- Secret des affaires
  - Diverses propositions législatives non abouties
  - Directive européenne à transposer

Risques PPST

www.cnrs.fr

- Les 4 risques au titre de la PPST
  - R1 : intérêts économiques de la nation
  - R2 : arsenal militaire = renforcer l'arsenal militaire d'un autre pays ou affaiblir les capacités de défense de la nation
  - R3 : prolifération = armes de destruction massives (nucléaire, balistique, chimique, biologique) et leurs vecteurs
  - R4 : terrorisme, y compris radiologique (bombe sale)
- 4 niveaux de risque de 0 à 3
- Dans la PPST tout repose sur une appréciation des risques



Risques PPST

www.cnrs.fr

- Zone à régime restrictif (ZRR)
  - Périmètre avec signalétique
  - Contrôle d'accès
  - Mesures concernant les visites
  - PSSI
- Locaux sensibles
  - Au sein d'une ZRR
  - Risques accrus (R3 et R4) → protection renforcée
- Secteurs scientifiques protégés
  - N'est plus lié au lieu mais au secteur d'activité
  - Quasiment tous sauf SHS

PPST, le cas du numérique

www.cnrs.fr

- Objectifs de la PPST :
  - Empêcher, à partir de ces locaux et terrains clos, la fuite d'informations
  - Prévenir le détournement d'informations scientifiques ou techniques sensibles
- Le numérique
  - Réduit à la portion congrue dans le texte
  - Mêmes mesures pour le physique et le numérique
  - Attention particulière aux solutions d'externalisation
  - Mise en place d'une PSSI
- Accès à distance ou virtuel
  - Mêmes règles de contrôle d'accès que pour l'accès physique
  - Autorisation par le chef de service et conformité à la PSSI
- Comment fait-on ?

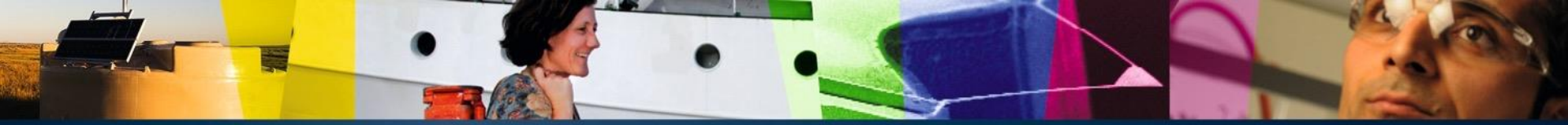
www.cnrs.fr

Normes, standards et référentiels

Normes, standards et référentiels

www.cnrs.fr

- Normes
  - International (ISO), national (AFNOR)
  - Fruit d'un consensus
  - Reconnaissance large et forte valeur juridique
- Standard
  - Norme de fait
  - Autorité moindre du producteur
- Référentiel
  - Publié par différents organismes
    - De l'agence gouvernementale (ANSSI) à une société privée
  - Il en existe d'excellents



Que doit faire un développeur ?

www.cnrs.fr

- S'appuyer autant que possible sur des normes, standard et référentiels reconnus
  - Ne pas chercher à réinventer la roue

www.cnrs.fr

Homologation

Homologation

- RGS
  - *La décision d'homologation atteste, au nom de l'autorité administrative, que le système d'information est protégé conformément aux objectifs de sécurité fixés et que **les risques résiduels sont acceptés**.*
- PSSIE
  - *L'homologation est l'acte selon lequel l'autorité atteste formellement auprès des utilisateurs que le système d'information est protégé conformément aux objectifs de sécurité fixés. […] Cette décision s'appuie sur **une analyse de risques adaptée aux enjeux** du système considéré, et précise les conditions d'emploi.*
- ISO 27001:2011
  - *L'organisation doit appliquer un processus de traitement du risque de sécurité de l'information pour : obtenir du propriétaire des risques **l'approbation du plan de traitement du risque et l'acceptation des risques résiduels** de sécurité de l'information*

www.cnrs.fr

Licences et propriété intellectuelle

Problématique des licences

www.cnrs.fr

- Une application intègre très généralement des composants tiers, elle a été construite avec des outils de développement.
  - Chacun de ces éléments possède sa licence qu'il faut impérativement respecter
  - Il peut y avoir des incompatibilités entre ces différentes licences
- Quelques questions
  - Redistribution possible ?
  - Licence contaminante ?
  - Reverser les développements à la communauté ?
  - Attention à l'usage
    - Professionnel n'est pas personnel
    - Enseignement n'est pas recherche
- Choix d'une licence pour la distribution de l'application
- Régler les problèmes de licence avant d'entamer le projet
  - Choisir un autre composant si licence incompatible
- Intranet CNRS
  - https://intranet.cnrs.fr/Cnrs_pratique/juridique/proteger-vos-oeuvres/logiciels/Pages/default.aspx

www.cnrs.fr

Déclaration d'incidents

Déclaration d'incidents

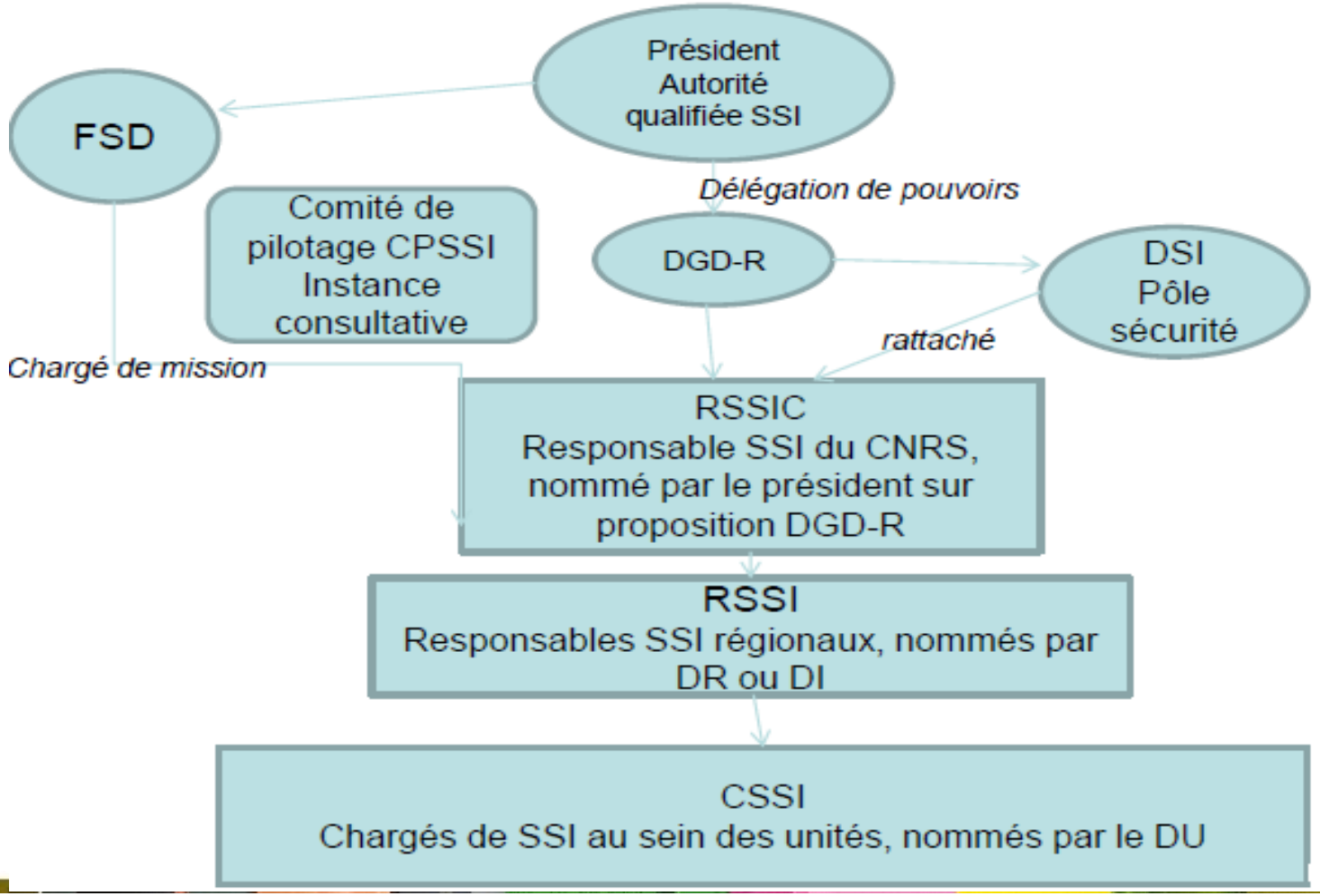
- Obligation
  - RGPD
  - PPST
  - LPM pour les OIV (non directement concerné au CNRS)
- Nécessité
  - Indicateurs pour suivre la sécurité
  - Corrélation
  - Détections de signaux faibles
  - Mise en place de mesures proactives pour contrer des attaques analogues
  - Protection juridique
- Outil de déclaration
  - https://extra.core-cloud.net/collaborations/RSSI-CNRS/SitePages/Déclarer%20un%20incident.aspx

www.cnrs.fr

Chaîne SSI

Organisation SSI au CNRS

www.cnrs.fr



Vade mecum du développeur

www.cnrs.fr

Que doit faire un développeur ?

www.cnrs.fr

- S'assurer en amont du projet du respect de la législation et de la réglementation
- S'assurer du respect des différentes licences et plus généralement de la propriété intellectuelle
- Prendre en compte la sécurité du début du projet jusqu'à l'arrêt de l'application
- S'appuyer sur des normes, standards et référentiels reconnus
- Maintenir une documentation → preuve
- Prendre conseil auprès des différents services du CNRS
  - CIL
  - DAJ
  - RSSI

www.cnrs.fr

Questions ?