RGPD, NIS2

deux mondes différents et pourtant complémentaires.

Table des matières

(*) glossaire page 9

CH17-RGPD

16 rue des raisins
17430 Tonnay-charente
e-mail : contact@ch17.rgpd.fr
tph : 0673955452

RGPD, NIS2

deux mondes différents et pourtant complémentaires.

1 Préambule :

Bienvenue,

Si vous parcourez cet article c'est que vous êtes soumis à la problématique suivante.

Le RGPD(*) qui s'applique depuis le 25 mai 2018 vous a demandé des efforts conséquents pour sa mise en place,

tant dans le domaine financier que dans la charge de travail.

Vous avez mis en place les mécanismes requis pour ce règlement et maintenant vous êtes confronté à l'application future de la nouvelle directive NIS2(*) qui entrera en application dès le mois d'octobre 2024.

L'empilement des Règlements et Directives vous semble insurmontable.

Le problème est posé, mais que faire pour gérer cet ensemble de la manière la plus efficiente possible ?

Nous allons vous guider et détailler notre vue de la façon la plus simple possible afin de mutualiser vos actions et utiliser ce qui existe déjà. Souvent par manque de dialogue entre les équipes, vous êtes amené à refaire ce qui existe déjà.

Pour réaliser ceci nous disposons de plusieurs avantages qui font notre particularité :

- Une expérience de **RSSI(*) de plus** de **18 ans**
- Une expérience de **DPO(*) externalisé de 4 ans**
- Une expérience de **Formateur Cybersécurité et Réseau** de **plus de 8 ans**.

Ceux-ci nous permettent de vous accompagner dans la gouvernance de votre mise en conformité NIS2 et RGPD.

Mais en réalité, à qui s'applique cette nouvelle directive ?

Regardons ce que nous stipule l'article 2 de la nouvelle directive NIS2.

« La présente directive s'applique aux entités publiques ou privées d'un type visé à l'annexe I ou II qui constituent des ***entreprises moyennes en vertu de l'article 2 de l'annexe de la recommandation 2003/361/CE****,* ***ou qui dépassent les plafonds prévus au paragraphe 1 dudit article****,* ***et qui fournissent leurs services ou exercent leurs activités au sein de l'Union.*** *»*

Ainsi que l'article 2 de l'annexe de la recommandation 2003/361/CE :

1. La catégorie des micro, ***petites et moyennes entreprises (PME)*** *est constituée des entreprises qui occupent* ***moins de 250 personnes*** *et dont le* ***chiffre d'affaires annuel n'excède pas 50 millions d'euros*** *ou dont le total du b****ilan annuel n'excède pas 43 millions d'euros.***

(*) glossaire page 12

CH17-RGPD

16 rue des raisins
17430 Tonnay-charente
e-mail : contact@ch17.rgpd.fr
tph : 0673955452

2. Dans la catégorie des PME, une petite entreprise est définie comme une entreprise qui occupe moins de 50 personnes et dont le chiffre d'affaires annuel ou le total du bilan annuel n'excède pas 10 millions d'euros.

3. Dans la catégorie des PME, une microentreprise est définie comme une entreprise qui occupe moins de 10 personnes et dont le chiffre d'affaires annuel ou le total du bilan annuel n'excède pas 2 millions d'euros.

Si vous entrez dans la définition d'une entreprise moyenne identifiée ci-dessus, la directive NIS2 s'appliquera à la condition d'être positionné dans un des secteurs d'activité figurant dans les annexes I et II de cette directive.

Attention, il existe toutefois des cas ou la taille, le chiffre d'affaire ne sont plus des critères déterminants, la directive s'applique elle aussi :

Nous trouverons dans ces cas étendus :

- *des fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public;*
- *des prestataires de services de confiance;*
- *des registres des noms de domaine de premier niveau et des fournisseurs de services de système de noms de domaine;*
- *une entité , dans un État membre, seul prestataire d'un service qui est essentiel au maintien d'activités sociétales ou économiques critiques;*
- *une perturbation du service fourni par l'entité pourrait avoir un impact important sur la sécurité publique, la sûreté publique ou la santé publique;*
- *une perturbation du service fourni par l'entité pourrait induire un risque systémique important, en particulier pour les secteurs où cette perturbation pourrait avoir un impact transfrontière;*
- *l'entité est critique en raison de son importance spécifique au niveau national ou régional pour le secteur ou le type de service en question, ou pour d'autres secteurs interdépendants dans l'État membre;*
- *une entité de l'administration publique (centraux ou régional).*

Cette nouvelle directive concernera désormais un domaine de compétence beaucoup plus étendu qui s'adapte à la situation de la cybersécurité et des attaques qui en découlent. Cette nouvelle contrainte a le mérite de s'adapter au mieux aux cyberattaques.

Afin de confirmer l'appartenance d'une entité à un cas étendu, il sera nécessaire de répondre aux conditions énoncées.

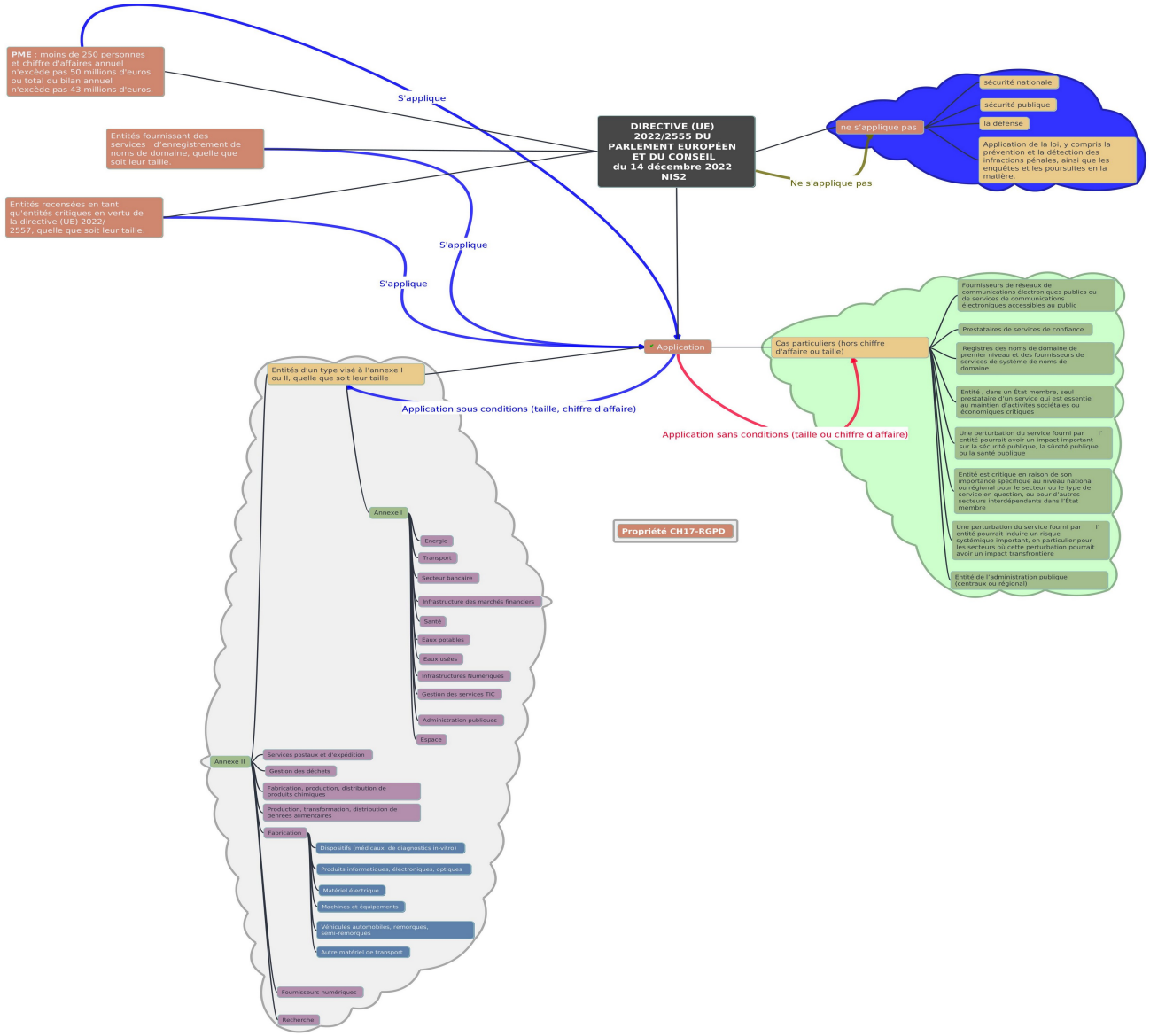
Pour tenter de simplifier voici les informations issues des annexes I et II de la directive qui détaillent les secteurs concernées. Nous vous conseillons de consulter les annexes afin d'obtenir les détails complémentaires quand ils sont cités.

(*) glossaire page 12

CH17-RGPD

16 rue des raisins
17430 Tonnay-charente
e-mail : contact@ch17.rgpd.fr
tph : 0673955452

Représentation graphique des domaines d'application :



(*) glossaire page 12

CH17-RGPD

16 rue des raisins
17430 Tonnay-charente
e-mail : contact@ch17.rgpd.fr
tph : 0673955452

Annexe I : Secteur hautement critique Entités Essentielles(*).

Secteur	Sous-secteur	Type
Énergie	Électricité	Fournisseurs, gestionnaires (distribution ou transport),producteur, opérateurs.
	Réseau de chaleur et de froid	Opérateurs de réseaux.
	Pétrole	Exploitants (oléoduc, production), centrales de stockage.
	Gaz	Entreprise, gestionnaire (distribution, transport, stockage, GNL), exploitant, raffinage.
	Hydrogène	Exploitants, stockage, transport
Transports	Aérien	Transporteurs, gestionnaires d'aéroports, contrôle de la circulation aérienne.
	Ferroviaire	Entreprise, gestionnaires d'infrastructures.
	Maritime	Sociétés, entités gestionnaires des ports,exploitants de service maritimes.
	Routier	Autorité routières, exploitants de systèmes de transports.
Secteur bancaire		Établissements de crédits
Infrastructure des marchés financiers		Exploitants de plateformes de négociations, contreparties centrales.
Santé		Prestataires de soins et de santé, laboratoires, recherche et développement, fabricant (produits pharmaceutiques, dispositifs médicaux).
Eau potable		Fournisseurs et distributeurs d'eau.
Eaux usées		Collecte, traitement des eaux.
Infrastructure numérique		Fournisseur (point d'échange internet, service DNS, informatique en nuage, centres de données, réseaux de diffusion de contenus, réseaux de communication public, service de communication accessibles au public). Prestataire de service de confiance.
Gestion des services TIC (inter-entreprises)		Fournisseurs (services gérés, service de sécurité gérés).
Administrations publiques		Entité de l'administration des pouvoirs public centraux.
Espace		Exploitants d'infrastructures terrestres (fourniture de services spatiaux).

(*) glossaire page 12

CH17-RGPD

16 rue des raisins
17430 Tonnay-charente
e-mail : contact@ch17.rgpd.fr
tph : 0673955452

Annexe 2 : Autres secteurs critiques Entités Importantes(*).

Secteur	Sous-secteur	Type
Services postaux et d'expédition		Prestataires de services postaux.
Gestion des déchets		Opération de gestion des déchets.
Fabrication production, distribution de produits chimiques		Fabrication, distribution, mélanges de substances chimiques.
Production, transformation,distribution de denrées alimentaires		Entreprises du secteur alimentaire (distribution en gros, production et transformation industrielle).
Fabrication	Dispositifs (médicaux, de diagnostics in-vitro)	Dispositifs médicaux.
	Produits informatiques, électroniques, optiques	Entreprises exerçant l'une des activités économiques visées dans la division 2 du document suivant.
	Matériel électrique	Entreprises exerçant l'une des activités économiques visées dans la division 27 du document suivant.
	Machines et équipements	Entreprises exerçant l'une des activités économiques visées dans la division 28 du document suivant.
	Véhicules automobiles, remorques, semi-remorques	Entreprises exerçant l'une des activités économiques visées dans la division 29 du document suivant.
	Autre matériel de transport	Entreprises exerçant l'une des activités économiques visées dans la division 30 du document suivant.
Fournisseurs numériques		Place ou moteur de marché en ligne.
Recherche		Organismes de recherche.

2 RSSI, DPO deux mondes qui se côtoient :

En réalité, les deux textes poursuivent le même but, protéger votre société d'une attaque, une compromission de votre système d'information ou de vos données personnelles.

Sur le fond ils sont en accord.

Par contre la forme change la donne, les rôles sont différents.

(*) glossaire page 12

CH17-RGPD

16 rue des raisins
17430 Tonnay-charente
e-mail : contact@ch17.rgpd.fr
tph : 0673955452

Le DPO

Il assure avant tout la Protection des Données Personnelles, participe à la libre circulation des mêmes données personnelles et assure le rôle d'interface entre :

- Le responsable de traitement (*)
- La CNIL
- Les utilisateurs

Le RSSI

Il est le garant de la Sécurité du Système d'Information.

Nous attirons ici l'attention sur la notion de système d'information.

Il s'agit de tout support qui participe au traitement de l'information.

Il ne se limite donc pas à un simple système informatique mais englobe donc bien tout (informatique ou non).

C'est pourquoi par exemple vous entendrez entre autres parler de mesures techniques et organisationnelles qui accompagnent des actions de mise en conformité.

3 Quels sont les rôles ? :

Chaque domaine dépend d'une **A**utorité de **C**ontrôle (**A.C**). (*)

En France pour le RGPD, il s'agit de la CNIL.

Pour la future directive NIS2 toujours en France c'est l'ANSSI qui gère.

Par extension, pour chaque membre de l'U.E c'est l'A.C du pays membre qui gère.

Vous trouverez les informations ci-dessous :

RGPD	NIS 2
Liste des A.C.	Présentation du réseau EU-Cyclone(*)

Il existe des similitudes car les deux autorités de contrôle disposent de prérogatives communes (exercées séparément bien sur), telles que :

- Inspections, contrôles sur place ou à distance ;

(*) glossaire page 12

CH17-RGPD

16 rue des raisins
17430 Tonnay-charente
e-mail : contact@ch17.rgpd.fr
tph : 0673955452

- Audit(*) (appelé Analyse d'Impact en RGPD celui-ci peut être transmis à la CNIL si le besoin est avéré) ;
- Accès à l'Accountability(*) et sa gestion pour les **RT(*), E.E(*)** ou **E.I(*)**.

Bien sûr n'oublions pas la partie sanctions applicables par les deux A.C.

Celles-ci doivent être proportionnées et dissuasives.

En se basant sur les textes officiels, les mécanismes de sanctions financières se ressemblent, par contre les montants diffèrent.

En RGPD, les sanction maximales en fonction de l'absence de respect d'obligation sont de :

- 2 % du C.A annuel ou 10 M€ ;
- 4 % du C.A annuel ou 20 M€.

avec en amont des mécanismes intermédiaires tels que :

- injonction
- astreinte financière

et en dernière arme ultime la suspension du traitement en cause.

Dans la directive NIS2, les plafonds identifiés sont actuellement de :

- 2 % maxi du C.A annuel pour une E.E
- 1,4 % maxi du C.A annuel pour une E.I

Pour information E.I et E.E sont définis dans l'article 3 de la directive NIS2 disponible ici.

Le périmètre de sanction NIS2 n'est pas encore affiné, l'ANSSI diffusera prochainement des informations complémentaires au plus tard en octobre 2024.

4 Quelles actions regrouper ?

Analyse d'Impact(*) versus Analyse de Risque(*) :

En terme RSSI, l'Analyse de Risque va réaliser l'état du niveau de sécurité d'un périmètre dédié de votre S.I.

Celle-ci sera réalisée à la demande de la société responsable auprès d'un organisme externe ou d'un auditeur interne habilité (*cas particulier d'un Lead Auditor interne*).

Son but est d'identifier les vulnérabilités et ainsi de parvenir à augmenter le niveau de sécurité d'un S.I pour rendre les risques acceptables en réalisant un audit d'un Système de Management de la Sécurité Informatique.

(*) glossaire page 12

CH17-RGPD

16 rue des raisins
17430 Tonnay-charente
e-mail : contact@ch17.rgpd.fr
tph : 0673955452

En terme RGPD, l'Analyse d'Impact apporte la preuve que le traitement réalisé n'est pas soumis à un risque excessif sur les données personnelles.

Le but est donc proche dans les deux cas, il faut protéger les informations personnelles ou les systèmes d'informations.

Si les buts sont proches, pourquoi ne pas fédérer les résultats disponibles en tenant compte du périmètre étudié ?

Prenons un cas pratique

Votre analyse de risque traite le transport des informations chiffrées entre le navigateur du client vers le serveur WEB (HTTPS/TLS) .

Pour les deux textes (RGPD et NIS2) ce mécanisme participe à la protection des données personnelles ou du transport des informations, de la gestion des accès (selon la vue du texte référencé).

Il peut donc tout à fait être cité dans chaque partie à condition d'être correctement documenté (accountability)(*).

Le but est donc bien d'utiliser ce qui existe déjà en respectant le RGPD et la directive NIS2 ***quand c'est possible*****.**

A l'inverse mener une analyse d'impact sur un traitement peut tout à fait servir de base pour une future analyse de risque **si celle-ci est menée dans les règles de l'art. Fédérer les deux est donc possible quand on fait attention au périmètre d'application.**

En généralisant ce raisonnement et après étude des critères communs entre RGPD et NIS2, il apparaît que les points suivants sont proches et peuvent être mutualisés sous les conditions énoncées supra :

RGPD	NIS2
Confidentialité	PSSI(*)
Intégrité	
Disponibilité	
Résilience	PCA / PRA(*)
Chiffrement	Crypto, Chiffrement(*)
Tests et analyses régulières	Évaluation par les pairs

5 Unification de la gestion quotidienne :

Chaque domaine de compétence impose des mécanismes tels que :

- Notification
- Supervision

(*) glossaire page 12

CH17-RGPD

16 rue des raisins
17430 Tonnay-charente
e-mail : contact@ch17.rgpd.fr
tph : 0673955452

- Contrôle

par et vers les autorités de contrôles.

L'intégralité de ces procédures peut tout à fait être mutualisée pour les deux domaines RGPD et NIS2.

Gestion de crise :

En période de crise disposer de procédures pérennes et claires représente un plus pour la société mise en cause.

Les mécanismes de gestion d'attaque ou de compromission restent les mêmes qu'ils soient vus en termes RGPD ou NIS2.

Il devient tout à fait possible de dégager des actions communes aux deux domaines et de ne traiter ensuite que les différences et particularités (par exemple la méthode de contact pour un **CSIRT**(*) en NIS 2 ou les obligations d'informations au utilisateurs pour une compromission de données personnelles en RGPD).

Globalement les processus d'analyses restent les mêmes.

Quand un incident est détecté il devra être

- Qualifié
- Confirmé
- Suivi de mesures de corrections (urgentes ou non)

La gestion d'une compromission de données personnelles par exemple dispose donc d'actions communes à la gestion d'une cyberattaque (seules celles-ci sont citées, les points particuliers n'y figurent pas ils seront gérés à part).

- Alerte
- Détection
- Identification
- Confirmation
- Correction(s)
- Retex.(*)

En fédérant les éléments communs en fonction des besoins de la société, il est possible de gagner du temps dans la gestion, la rédaction des procédures et donc de l'argent tout simplement.

(*) glossaire page 12

CH17-RGPD

16 rue des raisins
17430 Tonnay-charente
e-mail : contact@ch17.rgpd.fr
tph : 0673955452

6 Comment piloter cette unification ?

En principe le DPO ou la personne désignée devrait être formé en terme RGPD. (Art 37-5 du RGPD)

Le RSSI quant à lui sera formé en terme technique, organisationnel, la partie protection des données personnelles ne sera pas forcement sa priorité.

Il convient dans un premier temps d'analyser l'existant afin d'identifier les éléments communs.

A partir de ce constat, l'accompagnement du travail collaboratif peut commencer.

Chacun dans son domaine respectif apportera les éléments disponibles en respectant le droit d'en connaître.

C'est dans cet accompagnement que nous apportons nos services et mettons notre expérience à disposition :

- **Fédération de la Gestion des Risques ;**
- **Fédération des Obligations d'Informations et des Procédures qui en découlent ;**
- **Relation avec les Autorités de Contrôles ;**
- **Accompagnement des DPO, RSSI et Responsables de Traitements pour faciliter le travail collectif.**

Et bien sûr mise en Conformité Réglementaire en vertu de la Directive NIS2 ou du RGPD de manière plus générale.

7 Conclusion :

Le RGPD et la directive NIS2 disposent de parties communes qu'il est ainsi possible de fédérer pour gagner du temps et de l'argent.

Bien que les rôles soient séparés, des éléments communs existent.

Souvent des éléments restent sous-exploités par manque de connaissance ou de dialogue.

Notre expérience en tant que RSSI, DPO et Formateur Cybersécurité et Réseau (plus de 23 ans d'expérience au total) nous permet d'apporter une vue plus synthétique tout en respectant les contraintes imposées par ces deux textes.

L'objectif principal est de simplifier au maximum pour réduire l'effet d'empilement des règlements et directives qui vous semble un frein à leur mise en œuvre.

Merci de votre lecture.

(*) glossaire page 12

CH17-RGPD

16 rue des raisins
17430 Tonnay-charente
e-mail : contact@ch17.rgpd.fr
tph : 0673955452

8 Glossaire :

Accountability	*: o*bligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données.
Analyse de risque (informatique)	*: é*tude permettant d'évaluer l'ensemble des systèmes informatiques et de tous les processus associés afin de s'assurer de leur conformité aux normes, de leur fiabilité, de leur sécurité, et surtout de leur efficacité.
Autorité de contrôle (A.C)	: fournissent des conseils d'experts sur les questions liées à la protection des données et traitent les réclamations introduites relatives à des violations du règlement ou des directives.
Analyse d'impact	*:* étude qui doit être menée lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.
Chiffrement	*:* procédé de cryptographie qui consiste à protéger des données qui sont alors incompréhensibles pour celui qui ne dispose pas de la clef du chiffrement.
Crypto(graphie)	*:* la cryptographie est une technique d'écriture où un message chiffré est écrit à l'aide de codes secrets ou de clés de chiffrement.
CSIRT	*:* équipe de sécurité opérationnelle en charge de la réponse aux incidents de sécurité informatique.
DPO	*: personne* chargée de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'organisme qui l'a désigné pour l'ensemble des traitements mis en œuvre par cet organisme.
E.E	**: E**ntité **E**ssentielle identifiée dans l'annexe 2 de la directive,
E.I	**: E**ntité **I**mportante, identifiée dans l'annexe 1 de la directive.
EU-Cyclone	*:* réseau européen d'organisations de liaison en cas de crises de cybersécurité (UE – CyCLONe).
NIS2	*: NIS 2* (Network and Information Security, version 2) vise à harmoniser et à renforcer la cybersécurité sur le territoire européen.
PCA	*: Le plan de continuité d'activité (PCA ou, en anglais, Business Continuity Planning) vise à protéger l'ensemble des services de l'organisation. Ilintervient, en principe, en amont du PRA pour prévenir les incidents et en diminuer l'impact et la gravité.*
PRA	*:le Plan de Reprise d'Activité (* PRA), regroupe en amont toutes les mesures qui devront être appliquées, étape par étape, pour permettre aux utilisateurs du SI de retrouver l'accès aux données, aux applications, au réseau de l'entreprise et à internet.
PSSI	*: l*a politique de sécurité des systèmes d'information (PSSI) est un plan d'action défini pour maintenir un certain niveau de sécurité. Elle reflète la vision stratégique de la direction de l'organisme en matière de sécurité des systèmes d'information (SSI).
RETEX	*:* retour d'expérience qui recouvre les démarches et objectifs mis en œuvre pour résoudre un incident.. Il est souvent assimilé à un « débriefing ».
Responsable de Traitement (RT)	*: l*e responsable du traitement, est la personne qui décide des finalités du traitement et des moyens alloués pour le RGPD.
RGPD	*:* « Règlement Général sur la Protection des Données » (en anglais « General Data Protection Regulation » ou GDPR).
RSSI	*: l*e responsable de la sécurité des systèmes d'information surveille la définition et la mise en œuvre des politiques de sécurité de l'information de son entreprise.

(*) glossaire page 12

CH17-RGPD

16 rue des raisins
17430 Tonnay-charente
e-mail : contact@ch17.rgpd.fr
tph : 0673955452