OUTILS DE GESTION DES RISQUES ET AUDIT DE CONFORMITE A LA LOI SUR LA PROTECTION DES DONNEES PERSONNELLES

07 au 09 juin 2022
GOLDEN TULIPE
Cotonou

Par Ambroise Dj. ZINSOU Consultant formateur indépendant Management Télécoms & TIC et Protection des Données Personnelles et de la vie privée

AGENDA

A. ETUDE DES RISQUES

B. GUIDE DE CONDUITE D'AUDIT DE LA CONFORMITE

A. ETUDE DES RISQUES

I. Introduction

Dans le domaine des données personnelles, l'audit permet de vérifier dans quelles mesures, les directives du livre V ème du Code du numérique [Loi 2017-20 du 20 avril 2018] sont respectées par les organisations publiques ou privées pour se prémunir contre d'éventuelles sanctions . On parle d'audit de conformité.

L'audit de la conformité est une activité indépendante et objective qui donne à une organisation l'assurance sur le degré de maîtrise des opérations et de respect de la loi sur la protection des DP et qui lui apporte des conseils pour les améliorer, et contribuer à créer de la valeur ajoutée. L'audit aide l'organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle, et de gouvernance pour déterminer les écarts existants avec les points clés du code et d'établir une feuille de route pour la mise en œuvre de la conformité et en faisant des propositions pour renforcer leur efficacité.

Par ailleurs, l'audit de conformité est également un moyen d'améliorer la sécurité et la fiabilité du SI puisqu'il inclut également l'audit de sécurité informatique des données personnelles.

2. Enjeux

Les données à caractère personnel sont aujourd'hui à l'épicentre des enjeux de conformité rencontrés à travers le monde, profondément marqué par des cyberattaques de plus en plus fréquentes, nous rappelant à quel point les données personnelles sont une denrée convoitée. C'est ainsi que :

- En 2013, **TARGET**, une entreprise de grande distribution américaine, a été la cible d'un groupe de pirates qui lui ont dérobé les données personnelles de millions de clients dont la perte financière a été évaluée de 250 millions de dollars ;

- En 2015 le site **ASHLEY MADISON** spécialisé dans les rencontres extraconjugales a été attaqué. Les pirates menaçaient de dévoiler l'identité et les données de l'ensemble des clients du site. L'attaque a entrainé une série d'évènements dramatiques dont 4 suicides [celui d'un pasteur ayant été confirmé] avec à la clé des démissions de cadres dirigeants ;

- Le **PONEMON INSTITUTE**, dans le cadre de ses études indépendantes, a évalué le coût par donnée et par type d'incident. Ainsi, en 2017, le coût d'un dysfonctionnement informatique ou d'une erreur humaine représente

126 dollars par donnée compromise, celui d'une attaque malveillante étant de 156 dollars.

- Selon une étude du **BOSTON CONSULTING GROUP** datée de 2012, **« The value of our digital identity »**, les données personnelles des européens représenteraient 330 milliards d'euros par an pour les organisations publiques ou privées.

Et pourtant les organisations ne sont pas toujours conscientes des risques que courent aujourd'hui encore les données et en particulier les données personnelles.

La protection des données personnelles représente pourtant un défi majeur auquel les organisations doivent faire face et qui gagne du terrain. C'est eu égard à tout ce qui précède que la loi 2009-09 du 22 mai 2009 portant protection des données personnelles en République du Bénin a été remplacée par la loi 2017-20 du 20 avril 2018 portant code du numérique en république du Bénin pour tenir compte des nouveaux risques et défis en matière de protection des données personnelles.

3. Les sources d'harmonisation de la loi nationale :

- La Convention de l'UA sur la cybersécurité et la protection des données à caractère personnel du 23 juin 2014 qui vise à « renforcer et harmoniser les législations actuelles des Etats membres et des Communautés Economiques Régionales (CER) en matière de TIC dans le respect des libertés fondamentales et des droits de l'Homme et des Peuples ;

- L'Acte additionnel A/SA 1/01/10 du 16 février 2010 relatif à la protection des données à caractère personnel ;

- La Convention pour la protection des données à caractère personnel (STE N°108) ;

- Règlement général de protection des Données personnelles Européens ;

- La Constitution du Bénin 90 y compris ses révisions ;

- La loi 2009-09 du 22 mai 2009 portant protection des données personnelles en République du Bénin ;

- La loi 2017-20 du 20 avril 2018 portant Code du numérique en République du Bénin.

4. Les données personnelles : or noir du XXIème siècle

Avec le BIG DATA [Collecte massive de données personnelles] nait une autre forme d'exploitation des données personnelles celle de la collecte des données personnelles massives en vue d'un traitement pour des finalités ultérieures en fonction du marché des données. Il se définit comme un ensemble de « données structurées ou non dont le très grand volume requiert des outils d'analyse adaptés ». Le Big data représente une nouvelle terre de conquête et de développement pour les entreprises de sorte que certains parlent aujourd'hui d' « or noir du 21ème siècle » pour qualifier les données personnelles.

En effet, Les données souvent partagées entre plusieurs utilisateurs, sont de moins en moins localisées sur un serveur "local" et de plus en plus stockées dans le "**cloud**" (nuage), c'est à dire un espace "nébuleux", non identifiable, souvent réparti dans plusieurs centres dans le monde.

Outre les données volontairement enregistrées dans un "cloud" par les utilisateurs, toutes celles circulant sur le réseau internet sont systématiquement interceptées et collectées par des **robots informatiques** ["Bot"] qui scrutent inlassablement le cyberespace pour les incorporer dans le big data, vaste ensemble de données si volumineux qu'ils dépassent l'intuition et les capacités humaines d'analyse et même celles des outils informatiques classiques de gestion de base de données.

Le big data s'accompagne donc du développement d'**applications à visée analytique**, qui "**broient**" une multitude de données pour en tirer du sens.

5. Les risques attachés à la protection des données à caractère personnel

Les risques ont évolué en matière de protection des données à caractère personnel. Les vulnérabilités ne sont plus seulement attachées aux applications c'est-à-dire aux serveurs et aux réseaux mais elles atteignent les données essentielles à l'activité et les process.

5.1. Identification des risques

1. Risque d'image et risque business

La divulgation ou le vol de données qui ne sont pas assez sécurisées peut avoir un impact sur la confiance des clients et entamer profondément l'image de l'organisation.

Plus grave encore, le risque d'image étant lié au risque commercial, lui-même lié au risque sécurité, l'absence ou l'inefficacité de mesures de sécurité à la fois logiques et physiques peuvent entrainer la perte d'importants volumes de données personnelles

2. Risque juridique pour le Responsable du Traitement

Il s'agit des manquements du RT à ses obligations de sécurité des données personnelles. L'article 424 du CDN relatif à la sécurité du traitement énonce qu'en considération des risques que peut présenter le traitement « **….. dont le degré de probabilité et de gravité varie que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en oeuvre les principes relatifs à la protection des données, tels que la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent Livre et de protéger les droits de la personne concernée** ».

De même l'article 426 fait obligation au RT et son ST de mettre en oeuvre les mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, l'interception notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite

Ce risque potentiel que le RT se doit d'évaluer et de prévenir est d'autant plus crucial pour lui qu'en cas de non respect de ces obligations, celui-ci est susceptible de se voir appliquer des sanctions par l'APDP d'où la nécessité avant la mise en œuvre des traitements, de procéder à une analyse d'impact en application des dispositions de l'article 428 du CDN

3. Risque opérationnel

Depuis le dispositif **Bale II** [**Dispositif prudentiel destiné à mieux appréhender les risques bancaires**], le risque opérationnel est défini comme le risque de perte résultant des procédures internes, des membres du personnel ou de systèmes inadéquats ou défaillants, ou d'évènements extérieurs.
Les nouvelles règles du Code nécessiteront d'apporter une analyse sur l'organisation des systèmes d'information, et du pilotage. La mise en conformité nécessitera d'entreprendre une approche par les risques opérationnels pour permettre une meilleure gouvernance des données.
Les organisations devront notamment :

- Mettre en place des technologies automatisées associées à de nouvelles politiques notamment pour le respect des durées de conservation ;

- Déterminer des emplacements de stockage ;

- Agir en matière de sécurité informatique où l'impact sera particulièrement important. Les nouvelles exigences règlementaires vont nécessiter une refonte des processus opérationnels informatiques ainsi que de l'architecture des systèmes d'information, et de la gestion des programmes ;

- Permettre la formation des collaborateurs ainsi que le développement des nouveaux outils pour renforcer la collaboration entre le service informatique et les acteurs principaux de la protection des données à savoir le DPO, et l'APDP en vue de permettre un échange global d'informations.

4. Risque financier

Au-delà du risque juridique qui est attaché à des sanctions financières très lourdes, le risque financier est en réalité commun à tous ces risques et c'est finalement le risque financier qui permet véritablement d'apprécier l'ampleur et la portée des autres risques. Il est un risque indirect mais qui donne finalement **« l'état de santé de l'organisation »**.

Ce sont en effet les conséquences de l'atteinte au risque juridique qui peut être graves pour l'organisation et pas forcément le risque juridique en lui-même. Le risque d'image par exemple entraine une perte de légitimité et pour que l'entreprise « revienne », elle doit prévoir un budget conséquent pour redorer son image d'où un impact financier.

Son ampleur est difficile à évaluer, elle dépendra principalement du niveau de conformité à la loi

5. **Risque organisationnel**

Ce risque désigne un ensemble de **facteurs qui** influencent la performance opérationnelle. La notion de performance est ici multidimensionnelle : elle porte tout autant sur la productivité, que la qualité, la sécurité d'exploitation ou la sécurité au travail.

Le risque d'efficacité ou de performance est le risque lié à l'efficacité de l'exercice des activités, comme la productivité des processus et l'excellence opérationnelle, de manière à maintenir des coûts compétitifs. Ce risque est attaché à l'inefficience ou l'inadaptation des procédures qui peuvent avoir des impacts sur la mobilisation des ressources à la fois financières et temporelles de l'entreprise. Dans le contexte de la démarche de conformité, ces procédures ou étapes « inutiles » apportent de la lourdeur au programme de mise en conformité.

6. **Risque informatique**

Les atteintes aux systèmes d'information sont principalement de trois types. Il s'agit de :

- L'atteintes à la disponibilité ;
- L'atteintes à l'intégrité ;
- L'atteintes à la confidentialité.

Les risques trouvent leurs origines dans :

- Les causes accidentelles [Risques matériels, Pannes et dysfonctionnement de matériel ou de logiciel de base, ;

- Les erreurs humaines[Erreurs de saisie, de transmission et d'utilisation de l'information, Erreurs d'exploitation, Erreurs de conception et de réalisation, ;

- La malveillance [Vol et sabotage de matériel, Fraudes, Sabotage immatériel, Indiscrétion, détournement d'informations, Détournement de logiciels, Grève, départ de personnel stratégique, les attaques, etc….] .

5.2. HIERARCHISATION et EVALUATION DES RISQUES

L'identification, l'analyse et le classement des risques permettront de définir les actions de prévention les plus appropriées, couvrant les dimensions techniques, humaines et organisationnelles de l'organisation.

1. Mesure des risques identifiés

Les critères de classement des risques sont la probabilité qu'un problème survienne et l'impact qu'il aura sur le fonctionnement de l'organisation. Nous avons retenu cinq niveaux à chaque paramètre (Fréquence et impact). Ainsi donc à minima, deux critères sont appréciés pour coter le risque brut : la fréquence et l'impact :

Criticité (Risque brut) = Fréquence[probabilité]x Impact[gravité]

Les échelles d'évaluation permettent la hiérarchisation des risques et l'arbitrages sur les actions à mener.

i. La fréquence[probabilité]

La démarche consiste à estimer l'occurrence des événements pouvant être à l'origine des risques. L'échelle de mesure de la fréquence est établie et adaptée aux structures. Ci-après sont proposées l'illustration de mesure de la fréquence.

- Echelle de mesure de la fréquence

Cotation	Fréquence	Eléments de mesure
1	Très improbable	Occurrence quasi nulle [< 1%] sur 1 à 2 ans
2	Très peu probable	Occurrence possible mais peu probable [1 à 10%] sur 1 à 2 ans
3	Peu probable	Occurrence plausible mais peu probable [1 à 50%] sur 1 à 2 ans
4	Possible/probable	Occurrence probable [11 à _0%] sur 1 mois à 1 ans
5	Très probable à certain	Occurrence très probable [> 80%] sur 1mois à 1 ans

ii. L'impact[gravité]

Cotation	Impact	Probabilité
1	Mineur	Négligeable [< 10%]
2	Significatif	Probable 10 à 20%
3	Majeur	Hautement probable 30 à 49%
4	Critique	Prévisible 50 à 69s
5	Catastrophique	> 80%

iii. Côte des risques

Description	Cotation	Côte des couleurs
Mineur	1	
Significatif	2	
Majeur	3	
Critique	4	
Catastrophique	5	

2. L'Echelle de criticité

Elle permet de :

- Hiérarchiser les risques identifiés ;
- Choisir les actions jugées prioritaires pour envisager les mesures préventives ou correctives à mettre en œuvre aux fins d'agir de façon proactive face aux risques potentiels ;
- Maitriser et corriger les lacunes en prenant en considération le dégré de tolérance au risque de l'organisation défini au niveau de l'échelle d'appétence au risque qui suit :

Criticité (IxP)	Degré de classification de criticité	Description de la criticité
Catastrophique	Cr>17 Risque prioritaire	Impact catastophique. Arrêt du service rendu et des équipements. Impacts majeurs sur l'intégrité des installations. Plan des mesures d'urgence requis. Nécéssite une action immédiate ou faire couvrir le risque par une assurance. A traiter en priorité
Critique	13 ≤Cr ≤ 16 Risque à minimiser	Dégradation importante du service rendu et du fonctionnement des équipements. Plan d'action essentiel au fonctionnement critique des activités. A traiter avec un haut niveau de priorité nécessitant un plan d'action à court terme
Majeur	9 ≤Cr≤ 12 Risque à surveiller	Pertubation modérée des activités. Conséquences importantes sur l'efficacité des systèmes non compensables par les mesures correctives. Dégradation de l'environnement. Nécessite un plan d'action à moyen terme pour sa maitrise
Significatif	5≤Cr≤ 8	Efficacité réduite des systèmes en mesure d'être équilibrée par des investissements et une augmentation des dépenses opérationnelles.
Mineur	1<Cr≤ 4 Risque maitrisé	Impact limité. Pertubations mineures. Le risque se réalise rarement. Néanmoins un plan à long terme doit être envisagé

3. Établissement de la grille de criticité

L'impact[Gravité] et la Fréquence[Probabilité] permettent de déterminer la cotation brute ou inhérente du risque. A partir de l'échelle d'appétence, on peut remplir le graphe de criticité ainsi qu'il suit :

PROBABILITE						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		GRAVITE				

4. Registre des risques identifiés

Les risques identifiés sont :

- Risques d'image et risques business ;
- Risques juridiques ;
- Risques financiers ;
- Risques techniques ;
- Risques informatiques ;
- Risques organisationnels.
- Etc

5. Elaboration du registre des risques

- Le registre des risques à l'échelle de toute l'organisation se présente comme suit :

ID	Catégorie de risque	Détermination du risque		Evaluation du risque		Niveau de criticité du risque	Responsable	Actions	
		Dénomination	Conséquences	gravité	probabilité			Préventive	Corrective
	Financiers								
R1		Juridiques, sanction, fiscaux, sociaux Perte, de données Malveillance, Erreurs humaines, Perte de service essentiel	Non-respect de la réglementation, pénalités et perte de ressources	*5*	*5*	25			
	Informatique								
R2		les atteintes à la disponibilité, à l'intégrité et à la confidentialité	Arrêt de production, perte de revenu et de part de marché, Mauvaise qualité de services, inefficacité, protection inadéquate des données Perte de revenu, Perturbation de la production	*5*	*5*	25			
R3		Programmes Malveillants	Perte de revenu et Arrêt de production	*4*	*5*	20			
R4		Cyberattaques	Arrêt de production, perte de revenu et de part de marché	*4*	*5*	20			
	Opérationnels								
R5		Non protection des données personnelles et	Perte de revenu et d'image, liquidation	*4*	*5*	20			

		vie privée des usagers							
R6		Prestation de service des fournisseurs et équipementiers	Mauvaise qualité de services, inefficacité, protection inadéquate des données Perte de revenu, Perturbation de la production	4	4	16			
	ORGANISATIONNEL								
R7		Performance opérationnelle,	Contre performance productivité en baisse, la qualité exécrable, la sécurité d'exploitation ou la sécurité au travail compromis	4	3	12			
	JURIDIQUE								
R8		Poursuite judiciaire	Sanction, perte de revenu, e-réputation compromis, menace de liquidation	4	4	16			
R9		Non-respect de la législation et de la règlementation applicables au secteur d'activité.	Préjudice à la réputation et à l'image ; Pénalités en application des lois pertinentes : code du numérique, code du travail, code pénal, etc. Perte de ressources financières.	4	4	16			
	TECHNIQUES								
R10		Non respect des programmes et procédures de maintenance	Pannes récurrentes, vulnérabilité du SI, Perte de part de marché, chiffres d'affaires et d'image compromis.	4	5	20			

R11		Vol, Sabotage, fraudes au niveau des centres et des sites	Arrêt de production et perte de chiffre d'affaires	5	5	25			
R12		Dysfonctionnement du réseau	Perte de part de marché et de chiffre d'affaires et Mauvaise qualité de service	4	4	16			
R13		Inexistence d'un contrat d'assurance de protection des réseaux et locaux	Perte de l'image de marque, de marché et de Chiffre d'affaires	3	3	9			
R14		dysfonctionnement du système d'information (DSI)	Perte de revenu	4	3	12			

6. Détermination de la criticité des risques

Elle se calcule comme indiqué dans le tableau de criticité des risques évoqué ci-haut

7. Hiérarchisation des risques selon leur criticité

A partir des tableaux de criticité des risques, du registre des risques à l'échelle de toute l'organisation, la hiérarchisation des risques identifiés se présente ainsi qu'il suit :

PROBABILITE						
	5				R3, R4, R5,R10	R1, R2, R11
	4			R7,	R6,R8,R9,R12	
	3			R13	R14	
	2					
	1					
		1	2	3	4	5
		GRAVITE				

9.1. Risques à criticités élevées

ID	Catégorie des risques	Risque	Conséquences	Gravité	Probabilité	Criticité	Responsable	Actions préventive ou correctives
	FINANCIERS							
R1		Juridiques, sanction, fiscaux, sociaux Perte, de données Malveillance, Erreurs humaines, Perte de service essentiel	Non-respect de la réglementation, pénalités et perte de ressources	5	5	25		
	INFORMATIQUE							
R2		les atteintes à la disponibilité, à l'intégrité et à la confidentialité	Arrêt de production, perte de revenu et de part de marché, Mauvaise qualité de services, inefficacité, protection inadéquate des données Perte de revenu, Perturbation de la production	5	5	25		
R3		Programmes Malveillants	Perte de revenu et Arrêt de production	4	5	20		
	OPERATIONNEL							
R5		Non protection des données personnelles et vie privée des usagers	Perte de revenu et d'image, liquidation	4	5	20		
R4		Cyberattaques	Arrêt de production, perte de revenu et de part de marché	4	5	20		
	TECHNIQUES							
R10		Non respect des programmes et procédures de maintenance	Pannes récurrentes, vulnérabilité du SI, Perte de part de marché, chiffres d'affaires et d'image compromis.	4	5	20		

R11		Vol, Sabotage, fraudes au niveau des centres et des sites	Arrêt de production et perte de chiffre d'affaires	5	5	25		

L'ensemble de ces risques aura un impact catastophique sur l'organisme si l'un quelconque d'entre ceux identifiés venait à se produire. Pour l'éviter, un plan des mesures d'urgence est requis. Il nécéssite une action immédiate ou faire couvrir le risque par une assurance. Ces risques doivent être traités en priorité. En outre un minimum d'investissement est réquis [protection du système d'information contre toute forme d'attaques, protection des équipements contre le vol, le sabotage, remplacement des équipements obsolètes]. Il faut veiller au respect de la réglementation pour éviter des sanctions

9.2. Risques Critiques

ID	Catégorie des risques	Risque	Conséquences	Gravité	Probabilité	Criticité	Responsable	Actions préventive ou correctives
	JURIDIQUE							
R8		Poursuite judiciaire	Sanction, perte de revenu, e-réputation compromis, menace de liquidation	4	4	16		
R9		Non-respect de la législation et de la règlementation applicables au secteur d'activité.	Préjudice à la réputation et à l'image ; Pénalités en application des lois pertinentes : code du numérique, code du travail, code pénal, etc.	4	4	16		

			Perte de ressources financières.					
	OPERATIONNEL							
R6		Prestation de service des fournisseurs et équipementiers	Mauvaise qualité de services, inefficacité, protection inadéquate des données Perte de revenu, Perturbation de la production	4	4	16		
	TECHNIQUES							
R12		Dysfonctionnement du réseau	Perte de part de marché et de chiffre d'affaires et Mauvaise qualité de service	4	4	16		

9.3. Risques Majeurs

ID	Catégorie des risques	Risque	Conséquences	Gravité	Probabilité	Criticité	Responsable	Actions préventive ou correctives
	OPERATIONNEL							
R7		Performance opérationnelle,	Contre performance productivité en baisse, la qualité exécrable, la sécurité d'exploitation ou la sécurité au travail compromis	4	3	12		
	TECHNIQUES							
R13		Inexistence d'un contrat d'assurance de protection des réseaux et locaux	Perte de l'image de marque, de marché et de Chiffre d'affaires	3	3	9		
R14		dysfonctionnement du système d'information (DSI)	Perte de revenu	4	3	12		

B. GUIDE D'AUDIT, OUTILS TRANSVERSES POUR CONTROLER LE DISPOSITIF DE CONTROLE

Cette démarche d'audit s'appuie sur le livre V^{ème} du Code du numérique.
Le terme DP sera parfois utilisé pour désigner les données à caractère personnel ou données personnelles
Les termes ST et RT seront également employés pour désigner respectivement le sous-traitant et le responsable de traitement.

GOUVERNANCE					
Composante de contrôle interne	**Finalités ou objectifs de contrôle**	**Points de contrôle**	**Impacts**	**Bonne pratique de contrôle interne**	**Technique d'audit**
POLITIQUE	S'assurer que la protection des données personnelles est encadrée et clairement règlementée en interne	Politique de protection des données claire et diffusée aux acteurs de la protection des données en interne	Risque de désorganisation - Méconnaissance par les personnes de leurs droits	- Désigner une personne en charge de porter le dossier protection des données et la politique afférente	**-Analyse documentaire** : - Demander une copie de la politique et une trace mail prouvant la diffusion en interne - Vérifier si la politique est passée en Comex [comité exécutif ou Comité de Direction] : récupérer le compte rendu du Comex qui a validé la politique et sa diffusion
	S'assurer que la documentation (charte, guide de bonne conduite, procédures, note interne) est mise à jour et diffusée à l'ensemble du personnel de l'entreprise	- Documentation communiquée d'une manière adéquate et facilement accessible (intranet, newsletters, réseau social interne…)	Le personnel ne détient pas les informations lui permettant d'assurer la protection des données personnelles	Mettre en place une veille juridique pour maintenir la documentation à jour	- **Analyse documentaire** : - Vérifier que les documents à disposition des salariés sont facilement accessibles : site intranet du groupe, publications de l'entreprise, newsletters, rapports annuels - Demander les dernières procédures pour vérifier la mise à jour effective - **Sondage** : - Sélectionner un échantillon représentatif parmi le personnel à interroger sur leur connaissance de la documentation

Data Protection Officer [DPO]	-S'assurer que l'entreprise a nommé en interne une personne chargée de la protection des données ou désigné cette personne en tant que DPO à l'autorité de contrôle	- Vérifier si l'entreprise répond à l'un des cas de désignation obligatoire posés par le GDPR - Moyen de désignation formelle auprès de l'autorité de contrôle - Formalisation des missions du DPO: lettre de mission - Annuaire des DPO	- Risque de non-conformité au règlement - Risque de sanctions financières - Risque d'image et de réputation - Risque d'efficacité et de non atteinte des objectifs	- Mener une réflexion pour identifier une personne en charge de la protection des données personnelles - Etablir une procédure de nomination (interne) et/ou de désignation (externe) - Formaliser les missions confiées au DPO et les ressources dont il dispose - Préparer le plan de communication concernant le DPO - Mettre à jour l'annuaire des DPO en fonction des arrivées/départs - Prévoir une personne remplaçante en cas de période de congés du DPO	- **Analyse documentaire** - Obtenir une preuve formelle de la nomination du DPO (lettre de mission signée) et de la communication de sa nomination en interne ou une trace de sa désignation auprès de l'autorité de contrôle - Interview du DPO pour s'assurer de sa motivation
	-S'assurer que cette personne dispose des ressources adéquates à l'exercice de sa fonction	- Budget nécessaire à ses activités - Formations requises pour son expertise - Disponibilité nécessaire au plein exercice de ses missions	- Risque d'efficacité et non atteinte des objectifs - Risque de non-conformité au règlement - Risque de sanction financières - Risque d'image et de réputation	- Identifier les formations requises lors de l'entretien annuel de performance et planifier son calendrier de formation - Mettre en adéquation le budget avec les enjeux	- **Analyse documentaire:** - Obtenir copie de la feuille de présence aux formations - Demander communication du budget consacré à l'activité - Identification des formations suivies ou à venir - Obtenir trace, le cas échéant, des difficultés liées à l'exercice des

				et au vu du rapport annuel d'activité et des priorités de l'année en cours ou à venir - Prévoir d'organiser une réunion avec le RT pour échanger sur l'exercice de sa mission	fonctions du DPO (manque de disponibilités, manque de ressources) et le plan de remédiation associé
Relais du DPO	S'assurer que le DPO a identifié des relais compétents sur son périmètre le cas échéant (interlocuteurs privilégiés du DPO)	- Annuaire de la liste des relais - Lettre de mission des relais - Formations requises pour leur expertise - Disponibilité nécessaire au plein exercice de leurs missions - Intranet protection des données personnelles rendu accessible aux relais - Si nécessaire, justification de l'absence de relais	-Risque de désorganisation/d'efficacité : absence de visibilité sur les traitements en place si absence de relais sur le périmètre du DPO	- Cartographie des traitements et organigramme pour avoir une visibilité sur la répartition centralisée ou décentralisée des traitements (au sein des différentes directions) - Identifier une personne relais au sein de chaque direction - Etablir une procédure de nomination (interne) - Formaliser les missions confiées aux relais et les ressources dont ils disposent (budget consacré au développement des compétences) - Organiser la formation des relais - Préparer le plan de	-**Analyse documentaire:** Obtenir une preuve formelle de la nomination des relais (sélectionner un échantillon éventuellement) : annuaire, lettre de mission - Accéder à la cartographie des traitements - Identification des formations suivies ou à venir et trace, le cas échéant, des difficultés liés à l'exercice de ses fonctions (manque de disponibilité, manque de ressources) - **Entretien** avec quelques relais pour apprécier leur niveau de compétence et leur implication - Récupérer l'argumentaire le cas échéant (si absence de relais

				communication concernant les relais - Mettre à jour l'annuaire en fonction des arrivées/départs	
Pilotage de l'activité	- Vérifier que l'entreprise met en place des comités de suivi entre le DPO et les relais au sein des différents services	- Existence et fréquence des comités - Agenda et comptes rendus des comités - Diffusion/publication des comptes rendu par mail ou sur l'intranet de l'entreprise - Tableau de bord de suivi, reporting et préparation du bilan annuel d'activité	- Absence de pilotage et de maitrise de la protection des données : manque d'efficacité et perte de temps dans les décisions - Non pérennité de l'activité	- Identifier les membres du comité : prévoir la présence des acteurs de la protection des données - Mettre en place un planning des réunions de pilotage - Définir les indicateurs des tableaux de bord (par ex lettre de mission signée, nomination et /ou désignation des DPO, identification des relais…) - Mettre en place un calendrier de communication (visibilité sur les thématiques et échéances) - Prévoir au cours de ces comités de faire le point sur les ressources, les problématiques rencontrées…	- **Analyse documentaire :** - Récupérer la note de décision sur le comité (expliquant sa fréquence, ses missions…) - Demander les comptes rendus des 2 ou 3 derniers comités ainsi que les présentations - **Rapprochement**: Accéder au dernier bilan annuel d'activité et le confronter aux comptes rendus des comités de l'année concernée

conformité au CDN	- Vérifier que l'entreprise organise sa mise en conformité, lui permettant de s'assurer que toutes les activités prévues sont en adéquation avec les objectifs et la contrainte "temps" du projet de mise en conformité	- Existence et fréquence des comités de pilotage de la conformité : agendas et comptes rendus des comités - Diffusion/publication des comptes rendus par mail ou sur l'intranet de l'entreprise - Tableau de bord de suivi, et reporting - Budget - Liste des responsabilités dans le projet	- Pas de suivi de la mise en conformité - Risque juridique	- Identifier les membres du comité : Présence acteurs concernés par la conformité au Code - Mettre en place un planning des réunions de pilotage - Définir les indicateurs des tableaux de bord (par exemple inventaire des traitement, analyse d'écart, conformité juridique, conformité informatique…) - Faire le point sur les ressources, les problématiques rencontrées… - Mettre en place un calendrier d'exécution des activités et définir des étapes pour s'assurer que les objectifs initiaux sont réalisables - Recenser les ressources dont dispose l'entreprise dans la mise en oeuvre du projet	- **Analyse documentaire:** Récupérer la note de décision sur le comité - Demander les comptes rendus des 2 ou 3 derniers comités ainsi que les présentations - Identifier et interroger quelques sponsors du projet (représente le projet) pour s'assurer de leur implication
Accountability	- S'assurer que l'entreprise documente l'ensemble de	- Registre des traitements	- Risque juridique et risque d'image - Impact humain:	- Réaliser en amont un audit des traitements	- **Rapprochement :** dans le registre, demander l'accès à

	ses actions pour démontrer la conformité de ses activités de traitement par rapport au code	(automatisés et non automatisés) - Conformité des traitements, existence de la documentation associée et efficacité des mesures de protection prises - Déploiement des procédures telles que le privacy by design, PIA [Analyse d'impact relative à la protection des DP] certifications et codes de conduite	risque pour les droits et les libertés des personnes - Manque d'efficacité	et de l'existence des méthodologies (privacy by design, PIA…) - Prévoir des procédures autour de la conformité des traitements, de la mise en oeuvre et tenue d'un registre - Revue régulière de la documentation pour assurer une protection des données en continu - Sécuriser le registre des traitements et structurer le registre (traitements lié au fonctionnement de l'organisme et ceux liés à l'activité du service) - Mettre en place un suivi des traitements identifiés par service	quelques traitements où la conformité est assurée pour étudier les éléments et d'autres traitements pour lesquels la conformité est en cours , vérifier la documentation associée et les mesures prises - Vérifier le niveau de sécurité du registre : contrôle d'accès, chiffrement
Sensibilisation/ formation	S'assurer que l'entreprise dispose d'un dispositif de sensibilisation des collaborateurs à tous les niveaux de l'organisation et qu'un suivi y est associé	- Supports de sensibilisation/ formations - Documentation diffusée ou existence d'une plateforme e-learning	- Risque d'erreur et de mauvaise manipulation des données par les collaborateurs	- Sensibilisation par population : identifier les services qui nécessiteront des sensibilisations régulières ou particulières (CA ou Comex et services traitant de données	- **Analyse documentaire**: - Obtenir les supports de sensibilisation et de formation des collaborateurs à la sécurité des données personnelles - Demander les feuilles d'émergement aux informations et accéder au tableau de bord de suivi des

				sensibles RH, marketing...) - Prévoir une demi-journée de formation voire une journée en présentiel de ces collaborateurs en interne ou en externe - Insérer dans le dossier du nouvel arrivant, une note d'information sur la protection des données personnelles, ou dans la vidéo de présentation générale de l'entreprise - Définir des indicateurs : connaitre le nombre de bénéficiaires des formations, ou personnes participant aux e-learning et des indicateurs de satisfaction des participants - Organiser des ateliers qui pourraient se tenir lors de la journée mondiale de protection des données le 28 janvier - Prendre en compte	formations et sensibilisation, '- '- Analyse du dossier du nouvel arrivant et de la présentation générale de l'entreprise '- **Tester** la plateforme e-learning

				la culture de l'entreprise dans le choix des outils	
Communication	- S'assurer de la capacité de l'entreprise à maintenir l'attention sur la protection des données personnelles	- Supports de communication: newsletters, intranet et réseau social interne, forums de discussion… - Existence d'une communication du groupe adaptée à l'intention de l'ensemble des collaborateurs - Identification du DPO par les collaborateurs (référent)	- Risque d'erreur : le personnel ne peut pas se mettre à jour sur la protection des données ni poser de questions	- Informer le personnel sur l'existence de l'interlocuteur clé (DPO) - Mettre en place une veille sur les outils de communication pour les renouveler (application smartphone…) - Adapter l'information en fonction des populations visées et des outils de communication utilisés (en indiquant le destinataire si l'information est ciblée, et passer par la direction de la communication pour des informations plus générales qui touchent l'ensemble des collaborateurs) - Recourir à des outils novateurs : afficher des rappels d'une manière ludique sur	- **Tester:** Vérifier l'efficacité du support de communication en testant des mots clés (pour rechercher des publications) - **Analyse documentaire**: - Récupération des exemples de communication faites par la filière communication pour des informations générales, et sur les supports de communication directement - Analyser la fréquence des newsletters et l'utilisation faite des forums

				les écrans des couloirs ou des ascenseurs, distribution de flyers, faire apparaitre des émoticônes ou personnages sur l'écran aléatoirement	
Transparence et compétitivité	- S'assurer que l'entreprise rend visible de l'extérieur sa politique en matière de protection des données personnelles pour renforcer le niveau de confiance de ses clients et partenaires externes	- Politique disponible et facilement accessible par la presse ou les individus - Charte protection des données personnelles - Processus de diffusion	- Les tiers et parties prenantes (clients, individus...) ne sont pas informés de l'attention que l'entreprise porte sur les données - Perte de confiance et potentiellement de compétitivité	- Rédiger une note de compétitivité autour des données personnelles en interne (arguments) - Mettre en place un plan de communication autour du marketing de la compétitivité (pour suivre les actions réalisées en matière de compétitivité) - Identifier la personne en charge de ce sujet de compétitivité qui pourra être l'interlocuteur entre l'entreprise et les tiers - Mettre en place un formulaire de contact par lequel les tiers pourront contacter l'entreprise - Prévoir une politique de	- **Analyse documentaire**: - Accéder au plan de communication - Voir si le formulaire de contact est simple d'utilisation (onglet déroulant) et facilement accessible - Politique de communication en cas de crise - **Tester:** Consulter les publications et l'onglet réservé à la protection des données sur l'extranet de l'entreprise

				communication externe en cas de crise	

CONFORMITE DES TRAITEMENTS

Composante de contrôle interne	Finalités ou objectifs de contrôle	Points de contrôle	Impacts	Bonnes pratiques de contrôle interne	Techniques d'audit
Principe de licéité du traitement					
Finalité et qualité de la donnée	- S'assurer que l'entreprise a identifié des traitements et leurs finalités - S'assurer que la donnée est adéquate, pertinente et non excessive au regard de la finalité poursuivie, elle-même légitime et transparente	- Procédure permettant de déterminer la finalité d'un traitement et les données nécessaires à cette finalité - Chaque traitement fait bien l'objet d'une justification de sa finalité '- Pour chaque traitement, qualité des données ; données exactes complètes et mises a jour '- Formulaires de collecte ne contenant que les champs nécessaires	- Risque de non-conformité au code : sanction financière et atteinte à la réputation	- Limiter le partage en interne de documents contenants des DCP aux seules personnes ayant un besoin d'accès dans le cadre de leurs missions - Mettre en place une liste des données qu'il est possible de collecter et de celles qui ne doivent pas l'être, en fonction des services - Etablir des guides d'entretien qui permettent au DPO d'accompagner un service dans la mise en oeuvre d'un traitement (quoi collecter et dans quel contexte) - Encadrer les zones de commentaires: prévoir des cases à cocher ou menus déroulants,	- **Analyse documentaire**: - Vérification des formulaires de collecte et de l'existence et exhaustivité de la procédure - Pour quelques traitements en cours de production, demander les documents qui permettent de justifier les finalités et les données collectées Par exemple, pour les RH : regarder rapidement les dossiers du personnel pour s'assurer que des pièces inutiles n'y figurent pas (ex permis de conduire). Pour le service de la communication: aller

				vérifier régulièrement pour supprimer, listes de mots prohibés bloquant l'enregistrement du formulaire	voir le site internet - **Tester** les zones de commentaires
Conservation des données personnelles	- S'assurer que l'entreprise a défini des règles de conservation des données et de purge (ou archivage définitif)	- Existence d'une charte de définition et de gestion des durées de conservation prévoyant les modalités de conservation et celles d'archivage (courant, intermédiaire, définitif) Les durées sont issues de cette charte ou adaptées à la finalité du traitement - Le traitement intègre, si possible, la date de fin de conservation (ex pour un projet avec date de fin)	- Risque de non-conformité aux disposition du Livre V^{ème}: sanction financière et atteinte à la réputation	- La charte a été adaptée et déclinée pour chaque service - Faire un état des lieux de ce qui est sur le terrain - Permettre la suppression des données une fois le délai atteint : mettre en place un logiciel automatisé de suppression (jusque dans les sauvegardes et les archives) - Pour les données sensibles, prévoir des outils d'effacement sécurisés plus sophistiqués qu'une simple suppression - Mettre en place des règles d'accès aux archives en limitant cet accès aux seules personnes qui y ont intérêt - Mettre en place un système de protection physique	- **Analyse documentaire**: - Récupérer un exemple de charte déclinée - Pour un traitement : récupérer un exemple de durée de conservation, sa justification et la procédure associée à la purge

				des archives : badge, détecteur fumée…	
Respect des droits des personnes					
Recueil du consentement	- S'assurer que l'entreprise a recueilli le consentement de la personne préalablement au traitement de ses données dans le cas où le consentement est requis	- Existence d'une procédure de recueil du consentement diffusée en tenant compte des nouvelles arrivées - Par traitement concerné, collecte effective du consentement : existence d'un espace de collecte du consentement, traçabilité du consentement, et de son retrait	- Risque de non-conformité au GDPR : sanction financière et atteinte à la réputation	- Espace intranet de collecte ou case à cocher dans un contrat: "j'accepte la sollicitation" sur les formulaires en ligne	- **Analyse documentaire** : Vérifier la clarté et la diffusion de la procédure et accéder à la documentation applicable au traitement - **Test applicatif** de recueil du consentement
Droit à l'information	- S'assurer que l'effectivité des droits de la personne concernée est assurée par une information claire et accessible	- Procédure de gestion de l'information des personnes concernées faite au plus tard au moment de la collecte des données - Par traitement, définition des mentions d'informations et de leur mise en oeuvre là où c'est nécessaire (contrat, site intranet, e-mail, formulaire de collecte....) - Site de l'entreprise indiquant clairement la manière	- Risque de non-conformité au GDPR : sanction financière et atteinte à la réputation	- Prévoir des moyens permettant de démontrer que l'information a été donnée : case à cocher permettant de certifier que l'individu a été informé, faire signer un document de lecture des informations... - Identifier le ou les meilleurs moyens pour garantir l'information en amont de la collecte des données dont les informations sont	- **Analyse documentaire**: - Vérifier l'existence d'une procédure de gestion de l'information, sa clarté et sa diffusion - Sur un échantillon de traitements, vérifier que les mentions d'information sont dans les contrats de travail des collaborateurs et dans les conditions générales de vente et vérifier leur

		d'exercer ses droits : page d'accueil ou rubrique vie privée/données personnelles		amenées à être collectées : panneau d'affichage, mentions site web... - Informer la personne qui viendrait exercer ses droits, en cas de vidéosurveillance - Par téléphone, prévoir un message automatique avant la suite de la conversation offrant la possibilité de s'opposer à l'enregistrement lors d'une collecte OU donner la possibilité de sélectionner une touche pour plus d'informations sur les mentions	exhaustivité - Vérifier le site internet de l'entreprise
Exercice du droit d'accès des personnes concernées	-S'assurer que les personnes sont en mesure d'exercer leur droit d'accès dans les cas prévus par le règlement	- Procédure permettant de déterminer comment réceptionner la demande, à qui la transmettre, comment la gérer, qui répond, sous quel forme et dans le délai d'un mois - Exercice du droit d'accès automatisé ou manuel (adresse mail)	- Risque de désorganisation et absence de suivi des demandes - Pas d'interlocuteur désigné - Risque juridique (sanction et risque d'image)	- La procédure définit la bonne gestion du droit d'accès de la personne concernée, et est diffusée - Identifier la personne concernée - Prévoir d'envoyer un accusé de réception après réception de la demande - Automatiser dans les applications concernées l'exercice	- A**nalyse documentaire** : - Récupérer la procédure - Vérifier que le registre intègre bien des fonctionnalités permettant de suivre l'exercice des droits et les demandes en cours - Vérifier la clarté des réponses déjà apportées - **Tester** au

				du droit d'accès pour simplifier la démarche et tenir les délais (espace clients ou applications dédiées en interne) - Dans le cas contraire, mettre en place une adresse internet dédiée aux demandes d'accès (sur le site de l'entreprise) Dans ce dernier cas, désigner un service chargé de recueillir les demandes qui les redistribuera selon la demande en question - Mettre en place un outil de suivi des demandes afin de respecter le délai (ex le registre du DPO peut permettre le suivi de ce délai avec alerte intégrée) - Conserver la copie des démarches effectuées (copies écran, extractions…) - Tenir un journal de l'historique des demandes de droit d'accès (ex dans le registre du DPO)	niveau d'un traitement l'exercice du droit d'accès et vérifier la visibilité de l'adresse permettant à défaut de l'exercer

rectification, droit à l'oubli, droit à la limitation du traitement, et d'opposition	-S'assurer que les personnes sont en mesure d'exercer leur droit rectification, droit à l'oubli, droit à la limitation du traitement, et droit d'opposition	- Procédure globale permettant de déterminer comment réceptionner et traiter la demande, à qui la transmettre, comment la gérer, qui répond, sous quel forme et dans le délai d'un mois - Exercice manuel (adresse mail)	- Risque de désorganisation et absence de suivi des demandes - Pas d'interlocuteur désigné - Risque juridique (sanction et risque d'image)	- La procédure définit la bonne gestion des demandes de la personne concernée et est diffusée - Vérifier l'identité de la personne concernée, et définir l'organisation nécessaire à la réponse - Demander des justificatifs préalablement à la rectification : changement de statut pat, domicile. - Envoyer une capture d'écran à la personne concernée après rectification ou un message de confirmation de suppression - Désigner un service en charge de réceptionner les demandes qui les redistribuera au service pour traitement - Par voie électronique, prévoir une adresse mail ou un lien facilement accessible indiquant les éléments à transmettre	- **Analyse documentaire** : - Récupérer la procédure - Vérifier la visibilité de l'adresse mail - Vérifier le suivi des demandes en cours - Vérifier la clarté des réponses déjà apportées - **Rapprochement** au niveau d'un traitement : sélectionner des échantillons de demandes (rectification, effacement...) et les réponses apportées

Droit à la portabilité	- S'assurer que les personnes sont en mesure d'exercer leur droit à la portabilité	- Procédure globale permettant de déterminer comment réceptionner et traiter la demande, à qui la transmettre, comment la gérer, qui répond, sous quel forme et dans le délai d'un mois - Exercice du droit d'accès automatisé ou manuel (adresse mail)	- Risque de désorganisation et absence de suivi des demandes - Pas d'interlocuteur désigné - Risque juridique (sanction et risque d'image)	- La procédure définit la bonne gestion du droit à la portabilité et est diffusée - Vérifier l'identité de la personne concernée (si mode manuel) - Définir la nature des données concernées par la portabilité - Prévoir un système automatisé là où la portabilité est requise (ex B to C : énergie, assurance, banque, télécom...) pour simplifier la démarche et tenir les délais (espace clients ou applications dédiées en interne) - Dans le cas contraire, l'entreprise a mis en place une adresse internet dédiée à l'exercice du droit à la portabilité (sur le site de l'entreprise) - Désigner un service chargé de recueillir les demandes qui les redistribuera selon la demande en question - Envoyer un accusé de réception de la demande - Mettre en	- **Analyse documentaire** : - Accéder à la procédure - Vérifier les réponses déjà apportées - Vérifier la visibilité de l'adresse permettant à défaut d'exercer ce droit - **Tester** pour s'assurer que le registre intègre bien des fonctionnalités permettant de suivre l'exercice de la demande en cours - **Tester** au niveau d'un traitement l'exercice du droit à la portabilité

				place un outil de suivi des demandes afin de respecter le délai (ex le registre du DPO peut permettre le suivi de ce délai avec alerte) - Conserver la copie des démarches effectuées (copies écran, extractions…) - Tenir un journal de l'historique des demandes (ex registre du DPO)	
Obligation de notification	- S'assurer que l'entreprise organise l'obligation de notification de violation de données	- Procédure de notification des violations de données diffusée - Moyen électronique sécurisé pour la notification	- Risque de non-conformité au GDPR : sanction financière et atteinte à la réputation	- Sensibiliser particulièrement sur le sujet puisque la notification doit avoir lieu en tout état de cause - Mettre en place la procédure de communication à la personne concernée après évaluation de l'APDP sur l'impact de la violation - Puisque la loi n'impose pas de délai au sous-traitant, il conviendra de prévoir dans le contrat, les délais de transmission de la violation	- **Analyse**r: accéder à la procédure de communication - Sélectionner les contrats de quelques sous-traitants et vérifier la prise en compte de la notification - Trace de la sensibilisation particulièrement des SI
Transferts & Contrats					

Transferts	- S'assurer de l'encadrement du transferts des données hors UE	- Le registre du DPO identifie pour les traitements concernés par des transferts hors UE, le dispositif permettant de l'encadrer - Le contrat doit préciser le dispositif d'encadrement retenu pour les transferts	- Risque extraterritorial - Risque juridique : sanction financière et risque d'image - Risque d'efficacité	- Mettre en place une cartographie des flux de données - Disposer de BCR pour encadrer les transferts au sein du groupe - Référencer des sous-traitants qui ont leurs propres BCR ou qui ont adopté un dispositif pour le transfert de nature à protéger les données (ex Privacy Shield pour les Etats-Unis...)	- **Analyse documentaire**: - Accéder à quelques contrats - **Rapprochement:** Vérifier que les prestataires retenus ont des clauses contractuelles types signés selon le périmètre du transfert ou des BCR - Vérifier dans le registre que le transfert est bien identifié et que le dispositif d'encadrement y est rattaché (copie de la clause, copie de la certification...)
Contrats	S'assurer que les traitements confiés à un ST font l'objet d'une contractualisation	- Une clause spécifique à la protection des données personnelles est intégrée au contrat - Identification des ST - Le ST met en place des règles permettant de garantir la sécurité et la confidentialité des données ainsi que la destruction des données à l'issue de la mission - Registre et	- Risque juridique : sanction financière et risque d'image	- La clause de protection doit traiter le cas RT à ST et RT à RT (les périmètres de responsabilité de chaque RT devront être précisément indiqués dans le contrat) - La clause mentionne les obligations du ST, et les garanties à prendre (Sécurité, gestion des	- **Analyse documentaire : -** Vérifier l'existence de la clause spécifique (son exhaustivité) - **Rapprochement**: Pour un traitement, sélectionner un échantillon de contrats et la manière dont la clause a été intégrée et adaptée

		DPO (si cas de désignation obligatoire) pour les ST		données…), -Prévoir une clause de confidentialité et de réversibilité - Prévoir la possibilité de réaliser un audit des sous-traitants - Limiter l'accès aux données strictement nécessaires à l'exercice de sa mission et s'assurer qu'elles ne sont pas utilisées pour une autre finalité -Le contrat prévoit les conditions dans lesquelles les données doivent être soit détruites soit restituées a l'issue du contrat - Prévoir la validation des sous-traitants de 2ème niveau par le RT	
Privacy by design/ privacy by default					
Privacy by design/ privacy by default	- S'assurer que l'entreprise prend en compte la protection des données dès la conception du produit ou service et la décline pendant le traitement	- Existence de l'application d'une méthodologie de privacy by design/default	- Risque juridique - Risque d'efficacité	- Disposer d'une méthodologie de privacy by design qui assure l'instruction d'un traitement, sa conformité et sa contribution à l'accountability - La méthodologie doit	- **Analyse documentaire**: - Vérifier l'existence et l'exhaustivité de la méthodologie - **Rapprochement**; Pour un projet en cours de conception, vérifier la manière dont la

				permettre d'identifier la présence de données sensibles et de déterminer les mesures de sécurité appropriées, l'existence de transferts hors UE et de les encadrer avec le dispositif approprié, d'identifier les traitements à risque (qui pourraient exclure une personne d'un droit) - Prévoir un pack de formation des chefs de projets et des DPO à ces concepts - Lorsque nécessaire, la méthodologie privacy by design doit permettre de déclencher un DPIA	méthodologie est déroulée et les livrables associés
Analyse d'impact					
Analyse d'impact	- S'assurer que l'entreprise réalise une étude d'impact vie privée pour les traitements à risque	- Existence et application d'une méthodologie de DPIA - Cartographie des traitements ayant fait l'objet d'un DPIA ou devant faire l'objet d'un DPIA	- Risque juridique - Risque d'efficacité	- S'appuyer sur des experts externes pour réaliser les DPIA - Disposer d'une méthodologie pour laquelle les DPO et les RSSI ont été formés : la méthodologie doit prévoir la notification à l'autorité de contrôle	- **Analyse documentaire: -** Vérifier l'existence et l'exhaustivité de la méthodologie - Récupérer la cartographie - **Rapprochement**: Pour un projet en cours, de conception, vérifier la

				pour avis en cas de risque résiduel trop élevé - Etablir la liste des traitements identifiés par le G29[Groupe de travail 29] comme devant faire l'objet d'un DPIA et la relier aux traitements concernés en interne	manière dont la méthodologie est déroulée et les livrables associés
Contrôle de l'APDP					
Contrôle de l'APDP	- S'assurer que l'entreprise est organisée pour répondre aux contrôles de l'autorité de contrôle	- Procédure qui prévoit la manière d'agir et qui formalise les bonnes pratiques à adopter avec des contrôleurs - L'entreprise a désigné des personnes lors des contrôles de l'APDP et a établi la liste de ces personnes	- Réalisation du contrôle rendue plus difficile et relations plus délicates avec l'autorité de contrôle -Risque d'entrave au contrôle	- S'assurer que l'accueil est sensibilisé à la protection des données personnelles: demandes de réclamations ou contrôles - Informer l'accueil de ce qu'est l'APDP et comment agir face aux contrôleurs - La liste des personnes doit être présente à l'accueil - Prévoir un responsable des lieux qui coordonne le contrôle et sollicite les personnes qui y participent - Prévoir dans la procédure que le responsable des lieux vérifie la lettre de mission : agents, date,	- **Analyse documentaire** sur les bonnes pratiques et la procédure - **Interview** de l'accueil pour tester son aptitude face au contrôle - **Rapprochement**: Si des contrôles ont été faits: voir les documents produits lors de ces contrôles : prise de note (main courante), REX et si cela a été intégré dans la procédure

				périmètre - Prévoir d'appeler rapidement l'APDP pour vérifier qu'il s'agit bien un contrôle officiel contrôleurs dans les locaux - Prévoir une personne pour la prise de note - S'assurer que le responsable des lieux est sensibilisé en amont pour connaitre les droits de l'APDP en termes de contrôle : quels documents peuvent être demandés... - Faire appel à un expert éventuellement pendant la procédure de contrôle (avocat...) - Faire un retour d'expérience suite à un contrôle de l'APDP pour permettre des améliorations	

SECURITE INFORMATIQUE

Composante de contrôle interne	Finalités ou objectifs de contrôle	Points de contrôle	Impacts	Bonnes pratiques de contrôle interne	Techniques d'audit
Politique	- S'assurer que l'entreprise dispose d'une politique sécurité groupe et, le cas échéant, d'une charte informatique à jour qui prévoit les comportements des collaborateurs	- Une politique permet d'organiser la sécurité des SI - La politique est à jour et exhaustive	- Risque de mise en péril des SI - Risque financier et risque d'image - Risque opérationnel	- Diffuser des fiches thématiques ou politiques thématiques de sécurité, qui détaillent des éléments spécifiques tels que la politique mots de passe	- **Analyse : -** Vérifier l'existence et la pertinence de la politique groupe et analyser les fiches thématiques éventuelles:- vérifier la clarté des fiches thématiques et leur caractère synthétique - Vérifier la diffusion de la politique et sa visibilité sur l'intranet du groupe
	S'assurer que la politique et la charte font l'objet d'une diffusion	- Connaissance en interne de son existence et accessibilité	- Une méconnaissance de la politique entraine la mise en péril des SI - Risque financier et risque d'image - Risque opérationnel	- Diffuser régulièrement à titre de piqûre de rappel les exigences de sécurité - Donner un point de contact aux collaborateurs pour les accompagner dans l'application - Utiliser des réseaux interne, outils collaboratifs et newsletters	- **Analyse**: - Obtenir trace de leur diffusion
	Identification et authentification	- S'assurer que l'entreprise met en oeuvre des mesures sécures d'authentification afin	- Fichiers de journalisation - Pour chaque utilisateur, identité numérique unique et identification	- Usurpation d'identité et risque de fuite de données - Atteinte à la confidentialité des données, à la	- Adapter le niveau d'authentification en fonction de la sensibilité des données - Limiter les tentatives d'accès et historiser les tentatives -

		d'assurer la confidentialité des accès, la disponibilité des ressources et l'intégrité des données	obligatoire avant tout accès informatique	disponibilité des ressources et à l'intégrité des données	Mettre en place une politique de mot de passe : nombre et nature de caractères, changement régulier de mot de passe (par exemple trimestriellement) - Etablir une procédure de renouvellement de mot de passe en cas de perte et obligation de changement du MDP - Vérifier que les logiciels ne permet pas un enregistrement automatique des mots de passe - Prévoir le verrouillage des sessions automatique en cas de non utilisation pendant une certaine durée - Mettre en place un horodatage : date et heure de la dernière connexion au moment de la connexion à un compte
Gestion des habilitations / privilèges90	- S'assurer que l'entreprise a mis en place un mécanisme de définition des niveaux d'habilitation et d'un contrôle des accès	- Profils d'habilitations - Suivi des départs des salariés ayant un accès aux DCP ou le fait qu'un salarié ne soit plus habilité à accéder à un local ou à une ressource - Application du principe de moindre	- Risque d'accès et d'actions non autorisées par une personne ayant des responsabilités ou habilitations incompatibles sur les DCP	- Mettre en place une politique de contrôle des accès et la mettre à jour - Limiter les accès aux DCP aux personnes en ayant besoin dans le cadre de leur fonction - Prévoir la procédure à l'arrivée/départ d'une	- **Analyse documentaire**: - Accéder à la politique des accès et la procédure à l'arrivée/départ - Vérifier le tableau de suivi et trace des mises à jour éventuelles - **Rapprochement** : Accéder aux profils d'habilitation et

		privilège (accès aux ressources avec le minimum de privilèges pour conduire ses actions)		personne ayant un accès légitime aux DCP - Identifier clairement les personnes ayant un accès aux DCP et identifier les hauts privilèges et les justifier - Mettre en place un tableau de suivi des habilitations - Classifier les informations afin savoir où sont les données sensibles et les protéger en matière d'habilitation - Faire des revues régulières d'habilitations (voir qui à accès à quoi et si c'est légitime) - Réaliser une revue annuelle des privilèges pour identifier et supprimer les comptes non utilisé - Journaliser les informations liés aux privilèges -Tracer les accès pour suivre les activités des utilisateurs, les anomalies et événements liés à la sécurité.	s'assurer que leur gestion permet l'application du moindre privilège - vérifier pour quelques habilitations si les accès sont justifiés par la fonction de la personne (fiches de poste) - Vérifier que les tentatives d'accès sont suivies : demander un historique - Vérifier que le traçage des accès est sécurisé voir crypté

Recensement des applications	- S'assurer que l'entreprise recense ses applications	- Document permettant de connaitre en temps réel les applications régulièrement mis à jour	- Risque d'efficacité : mise en péril des SI	- Mise en place d'une cartographie des systèmes applicatifs - Mettre en place une collaboration entre les services pour récupérer les informations les plus justes possibles - Le document prévoit les applications contenants des DCP et trace les services les plus à risques et notamment les services traitements de données sensibles - Protéger les serveurs de manière physique : caméras et alarmes, portillon de sécurité et SAS accessibles par des dispositifs d'authentification (carte par exemple) - Revoir régulièrement les accès limités aux SAS ou locaux contenants des DCP et tenir un tableau de bord de ces accès - Entretenir la climatisation des locaux où sont stockées et traitées	- **Analyse documentaire**: cartographie des applications et accéder au document qui recense les applications contenant des DCP - **Interview** du RSSI sur comment la cartographie est rempli et mise à jour, et interroger sur la mise en oeuvre de la collaboration

				des DCP - Prévoir des moyens de protection contre les catastrophes naturelles (prévoir un générateur de secours en cas coupure électrique ou des sites de secours, faux plancher contre les inondations...) - Mettre en place de la maintenance	
Sécurité des flux et accès à distance	- S'assurer que les flux sont sécurisés	- Protocoles de sécurisation des flux	- Risque d'atteinte à la sécurité de la donnée si des fichiers sont captés lors de leur transfert	- Adapter le niveau de sécurisation des flux à la sensibilité des données - Utilisation du VPN pour les accès distants et chiffrement des données - Encadrer le télétravail	- **Analyse :** - Vérifier l'existence d'une cartographie des flux et des accès à distance - Obtenir le suivi les utilisateurs de VPN
Sauvegarde et continuité d'activité	- S'assurer que l'entreprise met en place des mesures de sauvegarde et de continuité de l'activité	- Système de sauvegarde des données et procédure associée - Existence d'un PCA	- Perte partielle ou totale des données	- Mettre en place une procédure de sauvegarde intégrant la destruction des sauvegardes une fois le délai de conservation ou d'archivage atteint - Redonder ses sites (avoir plusieurs sites : en réplication à chaud (copie en permanence) ou réplication à froid (réalisation de la copie	- **Analyse**: - Accéder à la procédure de sauvegarde - Demander les comptes rendus de test de continuité d'activité - **Tester** le PCA, et tester la procédure de sauvegarde

				à une fréquence définie), - Effectuer régulièrement des sauvegardes - Selon le volume de données, prévoir des sauvegardes incrémentales (n'enregistre que les modifications par rapport à une précédente sauvegarde) ou complètes à une fréquence moindre - Sécuriser le stockage des supports de sauvegarde - Réaliser des tests régulier de la continuité d'activité	
Gestion de crise/ gestion des failles de sécurité	- S'assurer que l'entreprise a un système de réaction suite à une faille de sécurité	- Existence d'un processus de gestion de crise - Système de supervision des SI	- Crise non contrôlée : impact financier et risque d'image - Risque juridique	- Prévoir une procédure de gestion des failles permettant de préserver les preuves de l'évènement, qualifier et corriger, réunir les bons interlocuteurs - Mettre en place des équipes spécialisées comme des centres de supervision de sécurité pour détecter en temps réel	- **Analyse**: accéder à la procédure de gestion des failles - Vérifier s'il y a des astreintes - **Interview** avec le RSSI et rencontrer les équipes spécialisées - Interroger le service informatique pour évaluer sa compétence de l'obligation de notification et obtenir éventuellement trace de la sensibilisation

				les tentatives d'attaque envers les SI - Inclure un volet sécurité au sein de chaque projet - Sensibiliser le service informatique à la transmission rapide de l'intrusion (si des DCP risque d'être atteintes) pour permettre au RT de procéder à l'obligation de notification	
Maintenance/ Support à distance	- S'assurer que l'entreprise fournit un support/assistance sécurisé à ses collaborateurs	- Suivi des opérations de maintenance - Sécurisation de la connexion lors du support - Script de support	- Risque de fuite des données - Impact opérationnel	- Enregistrer les opérations de maintenance - Tableau de bord de suivi des accès à distance - Configurer les outils de manière à recueillir le consentement de l'utilisateur avant la prise en main à distance (par exemple en cliquant sur une icône ou en répondant à un message s'affichant à l'écran) - Permettre à l'utilisateur de pouvoir constater si la prise en main à distance est en cours et quand elle se	- **Analyse**: - Vérifier l'existence d'une cartographie des incidents rencontrés - Accéder au suivi des opérations de maintenance et de supports à distance - **Tester** le support

				termine (affichage d'un message à l'écran) - Envoyer une confirmation par mail à la personne à la résolution de la panne - Tenir un suivi des accès à distance - Chiffrer les données de manière sécurisée avant envoi en maintenance externe de toute ressource informatique ou a minima faire signer un engagement de confidentialité au tiers prenant en charge le support	

La clé de la mise oeuvre sous contrôle de la conformité est une gouvernance fine et bien orchestrée, intégrant les notions de transversalité, de coopération, de complémentarité entre acteurs et de priorisation des actions.
Au regard des aspects techniques du règlement à maitriser, des travaux d'adaptation à réaliser, beaucoup d'entreprises en particulier pourraient ne pas parvenir à mettre en place ces changements seules. Inévitablement se posera la question de l'accompagnement externe notamment pour réaliser les diagnostics, les revues de conformité voir pour la conduite des missions d'audit sur les traitements et l'avancement des travaux.

JE VOUS REMERCIE