CEJM – BTS GESTION DE LA PME – 2e ANNÉE

THEME 4 – L'IMPACT DU NUMERIQUE SUR LA VIE DE L'ENTREPRISE

QUESTION 2 – Dans quelle mesure le droit intègre-t-il les questions liées au développement du numérique ? **CAS RGPD**

DROIT

Compétence : caractériser les conséquences juridiques des choix opérés par l'entreprise, sur la protection des personnes, des données.

Consignes

Ce cas, disponible sur l'ENT  ***dossier* CEJM TH4Q2*, est à traiter en groupe de quatre étudiants, en classe pour les questions sur les ressources notionnelles (dossier 1), sous forme de devoir maison donc à distance pour le cas et la synthèse (dossiers 2 et 3), qui feront l'objet d'une restitution en classe entière en présentiel.***

Vous pouvez créer un mur collaboratif  ***pour y partager vos idées et un pad***  ***pour y rédiger vos réponses (applications de l'ENT). Les travaux seront ensuite insérés dans un document créé sous texteur, puis déposé dans le dossier* CEJM TH4Q2 au format suivant : NOM ETUDIANT_CEJM_TH4Q2.**

Travail à faire :

Dossier 1 – Répondre aux questions sur les ressources notionnelles

Dossier 2 - Traiter le cas en rédigeant une note de synthèse

Dossier 3 - Rédiger l'essentiel de ce qu'il vous faut retenir du travail effectué

- *Définition des données personnelles et de l'identité numérique*
- *La nécessaire adaptation du droit*
- *Les grands principes du RGPD*
- *Le rôle de la CNIL*
- *Les impacts sur les organisations par les choix opérés par les entreprises sur la protection des personnes et des données*
- *Les conséquences juridiques de ces choix et les conséquences juridiques en cas de non-respect du cadre légal*

Contexte

GARAGE MARECHAL

Le garage Maréchal à Meillonnas dans l'Ain (01) est spécialisé dans les activités de mécanique automobile, carrosserie, vente de véhicules neufs (concession Renault) et d'occasion, dépannages, contrôles techniques.

Fiche d'identité

Date de création	1923
Fondateur	Clovis Maréchal
Dirigeant actuel	Fabrice Maréchal (petit-fils du fondateur)
Effectif	13 plus 1 (vendeur détaché par Renault)
Forme juridique	SARL
CA 2018	2 515 550 €
Siège social	320 route de Viriat - 01370 MEILLONNAS
2e établissement	16 chemin de la Carronnière – 01250 JASSERON
Site internet	https://www.garage-marechal.com/

Après un ralentissement en 2016, l'activité se développe (+5% de 2016 à 2017, +16% de 2017 à 2018). Elle génère beaucoup de déchets, c'est pourquoi le garage Maréchal, soucieux de l'environnement, a mis en place une organisation pour la gestion des déchets. En 2012, il a obtenu le label GARAGE PROPRE par la chambre des métiers de l'Ain. Ce label assure que des engagements ont été pris par le garage sur le recyclage des déchets, comme les peintures, solvants, huiles de vidange, filtres à huile, filtres à gasoil, batteries, mélange de carburant, pots catalytiques, carcasses de pneus, ferrailles, cartons, bidons d'huile vides.

Vous faites votre stage de 2e année dans le Garage Maréchal à Meillonnas (01). Fabrice Maréchal, le gérant, a quelques inquiétudes sur la conformité de l'entreprise aux règles du Règlement général de protection des données (RGPD), ***il vous a donc demandé de faire un rapport sous la forme d'une note de synthèse sur cette nouvelle réglementation, des impacts pour son entreprise et plus généralement sur de l'impact du RGPD sur une organisation***.

Pour réaliser votre rapport vous avez à disposition des ressources dans les dossiers suivants :

DOSSIER 1 : les ressources sur les notions

I. Données personnelles et identité numérique : de quoi s'agit-il ?

L'utilisation croissante d'internet dans les activités privées et professionnelles multiplie les occasions pour les individus de communiquer de façon volontaire ou involontaire, consciente ou inconsciente, des informations personnelles.

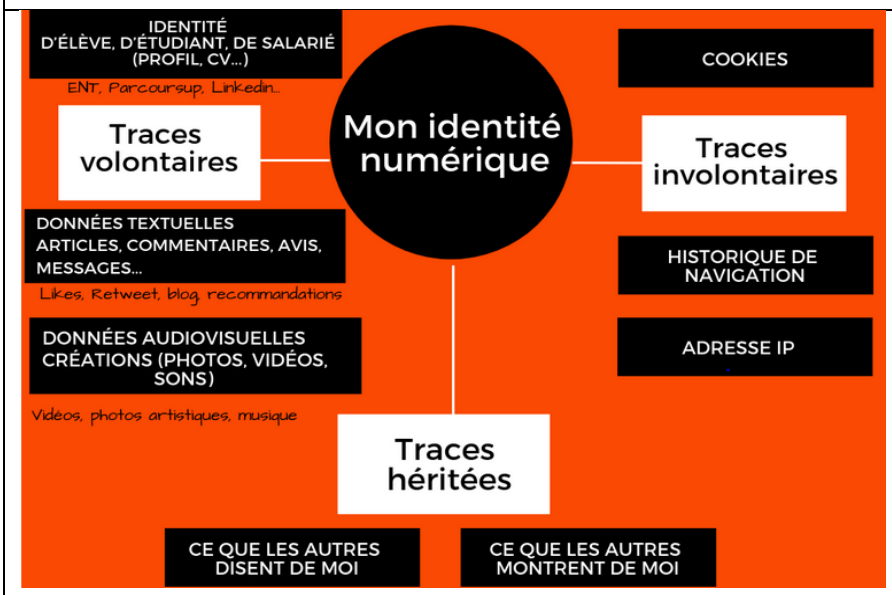
Les entreprises cherchent à collecter et conserver ces données qui ont une valeur considérable parce qu'elles leur permettent de mieux connaître leurs clients et de cibler leur offre.

Ressource 1 : QWANT – spot publicitaire : https://www.youtube.com/watch?v=Evahh1PXJIg

1.1 - Regardez la publicité pour le moteur de recherche Qwant proposée en ressource 1, et recensez les informations sur lui-même, communiquées au cycliste par le garde-forestier qu'il croise sur son chemin.

1.2 - Pour chacune de ces informations, indiquez à quelle occasion le cycliste a pu la laisser sur internet.

Ressource 2 : L'identité numérique



http://disciplines.ac-montpellier.fr/cdi/numerique/ressources-snt/thematique-les-reseaux-sociaux

1.3 - Classez les « traces » ainsi laissées par le cycliste sur le modèle du schéma de la ressource 2 : traces volontaires / traces involontaires.

1.4 - Reconstituez l'identité numérique du cycliste.

1.5 - En vous appuyant sur les ressources 1 et 2 et sur vos réponses aux questions 1.1 à 1.4, vous proposerez une définition de l'identité numérique.

Ressource 3 : La donnée personnelle - https://www.cnil.fr/fr/definition/donnee-personnelle

Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable. […] Une personne physique peut être identifiée :

- directement (exemple : nom et prénom) ;
- indirectement (exemple : par un numéro de téléphone ou de plaque d'immatriculation, un identifiant tel que le numéro de sécurité sociale, une adresse postale ou courriel, mais aussi la voix ou l'image).

L'identification d'une personne physique peut être réalisée :

- à partir d'une seule donnée (exemple : nom) ;
- à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour et membre dans telle association)

2 – D'après la définition officielle de la donnée personnelle (ressource 3), les traces numériques laissées par le cycliste peuvent-elles être considérées comme des données personnelles ? Justifiez votre réponse.

Ressource 4 : vidéo CASH INVESTIGATION – le marché colossal des données personnelles (oct 2015) https://actu.orange.fr/finance/videos/cash-investigation-le-marche-colossal-des-donnees-personnelles-CNT0000019o8R9.html

Ressource 5 : Qui exploite nos données personnelles ? (Ça m'intéresse – 27 juillet 2018)

[…] Encore plus forts, les réseaux sociaux. Pour récupérer des données personnelles, il leur suffit de se servir ! « Les déclarations au moment de l'inscription, et surtout les informations données au cours de leur utilisation, constituent une manne. Du coup, des acteurs comme Facebook ou Meetic peuvent se vanter d'être vertueux en matière de vie privée », ironise Fabrice Rochelandet. Certes, les conditions générales d'utilisation (CGU) fixent les règles mais « avec par exemple 60 applications, cela prendrait six mois de les éplucher », a calculé Benoît Thieulin, directeur de l'agence La Netscouade. […]

Les grands acteurs d'Internet, les fameux Gafa (Google, Amazon, Facebook, Apple), ne sont pas les seuls gloutons de la donnée. « Les banques ou des enseignes comme Carrefour en savent aussi beaucoup sur nous, précise Benoît Thieulin. Et les grandes plateformes qui gèrent ces données n'ont pas forcément un comportement plus éthique… »

En effet, dans ce paysage digital, des intermédiaires peu connus du grand public ont vu le jour. **Les sociétés de reciblage publicitaire, comme le géant Criteo, en font partie.** Leur métier consiste à recueillir des données de navigation personnelle – via les cookies – pour cibler les centres d'intérêt d'un individu. Un internaute qui a cherché un lave-linge verra s'afficher des bannières de publicité de lave-linge sur le site sportif qu'il consulte ensuite. Encore plus opaques sont les data brokers, ou courtiers en données. Ils vendent et achètent des fichiers en masse, les agrègent et les font parler. […] **Autre géant du secteur : Mediapost. Cette filiale de La Poste détiendrait 40 millions d'adresses postales, 26 millions d'adresses email et 19 millions de numéros de téléphone.**

Que font-ils de nos actes privés ? Le pire comme le meilleur. « Grâce à l'utilisation du big data, la santé va connaître un cycle d'innovations encore plus important que celui des antibiotiques », estime Benoît Thieulin. C'est la personnalisation des traitements qui est en jeu. Des applications mobiles de santé, notamment dans le diabète, ont aussi prouvé qu'elles amélioraient l'adhésion au traitement. **Mais le profilage de millions d'individus sert**

surtout à promouvoir des publicités ciblées, à peaufiner une offre de services… […]

Problème, ce travail de marketing ciblé peut se révéler terriblement intrusif. Preuve en a été donnée quand un père de famille américain, agacé que sa fille reçoive des bons de réduction pour des produits destinés aux jeunes mamans, a déposé une réclamation à son supermarché. Pourtant, l'arrivée dans la boîte aux lettres des coupons ne devait rien au hasard. Sa fille, encore mineure, était bel et bien enceinte. Son père l' ignorait mais une société spécialisée dans le data mining (l'exploitation de bases de données) l' avait découvert grâce aux produits que la jeune fille achetait. […] « Les citoyens ont donc raison de s' inquiéter, estime Benoît Thieulin. Le débat sur la protection des données doit avoir lieu. De cette manière nous éviterons des scénarios catastrophe tels que celui de la mutuelle qui augmente la prime d'assurance en fonction du comportement. »

3.1 - En quoi l'activité des nouveaux intermédiaires sur le marché du numérique comme Mediapost consiste-t-elle ? (Ressources 3 et 4)

3.2 - Quelles sont les utilisations possibles des données collectées ? (Ressources 4 et 5)

II. Protection des données personnelles : le droit s'adapte

Afin de préserver malgré tout les principes fondamentaux de droit au respect de la vie privée et du droit à l'image, le Droit a mis en place des moyens juridiques : règles et sanctions. Les entreprises doivent donc bien connaître le cadre dans lequel elles peuvent acquérir et utiliser les informations des internautes tout en respectant la réglementation de façon à éviter les sanctions.

Ressource 6 : Qu'est-ce que le RGPD ? https://www.cnil.fr/fr/rgpd-de-quoi-parle-t-on

L'acronyme RGPD signifie « Règlement Général sur la Protection des Données » […]. Le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne.

Le contexte juridique s'adapte pour suivre les évolutions des technologies et de nos sociétés (usages accrus du numérique, développement du commerce en ligne…).

Ce nouveau règlement européen s'inscrit dans la continuité de la Loi française Informatique et Libertés de 1978 et renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données les concernant. Il harmonise les règles en Europe en offrant un cadre juridique unique aux professionnels. Il permet de développer leurs activités numériques au sein de l'UE en se fondant sur la confiance des utilisateurs.

<u>Ressource 7</u> : Les grands principes des règles de protection des données personnelles (https://www.cnil.fr)

Quels sont les grands principes des règles de protection des données personnelles ?

Les 5 grands principes des règles de protection des données personnelles sont les suivants :

- **Le principe de finalité** : le responsable d'un fichier ne peut enregistrer et utiliser des informations sur des personnes physiques que dans un but bien précis, légal et légitime ;
- **Le principe de proportionnalité et de pertinence** : les informations enregistrées doivent être pertinentes et strictement nécessaires au regard de la finalité du fichier ;
- **Le principe d'une durée de conservation limitée** : il n'est pas possible de conserver des informations sur des personnes physiques dans un fichier pour une durée indéfinie. Une durée de conservation précise doit être fixée, en fonction du type d'information enregistrée et de la finalité du fichier ;
- **Le principe de sécurité et de confidentialité** : le responsable du fichier doit garantir la sécurité et la confidentialité des informations qu'il détient. Il doit en particulier veiller à ce que seules les personnes autorisées aient accès à ces informations ;
- **Les droits des personnes** (1)

(1) Principaux droits des personnes dont les données sont traitées :

Droit d'accès : avoir accès aux données ;

Droit de rectification : faire corriger des données inexactes ou incomplètes ;

Droit d'opposition : s'opposer à la poursuite du traitement les concernant ;

Droit à l'effacement : demander l'effacement de celles-ci sous conditions (données utilisées à des fins commerciales, non nécessaires au traitement, consentement retiré…) ;

Droit à la portabilité de leurs données : récupérer une partie des données pour pouvoir les stocker ou les transmettre en vue de leur réutilisation à des fins personnelles ;

Droit à la limitation du traitement : faire geler temporairement l'utilisation de ses données pendant qu'un autre droit (ex. rectification ou effacement) est étudié.

<u>Ressource 8</u> : RGPD : par où commencer ?

https://www.cnil.fr/fr/rgpd-par-ou-commencer

4 - Prenez connaissance des ressources 6 à 8 puis complétez le tableau ci-dessous, en proposant une action concrète par principe, pour une entreprise qui veut être en conformité avec le RGPD.

Application du RGPD : du principe à l'action

Principes	Actions
Finalité	
Proportionnalité et pertinence	
Durée de conservation limitée	
Sécurité et confidentialité	
Droits des personnes	

Ressource 9 : La CNIL – c'est quoi ? (https://www.cnil.fr)

La CNIL, c'est quoi ?

La **Commission Nationale de l'Informatique et des Libertés** (CNIL) a été créée par la loi Informatique et Libertés du 6 janvier 1978.

Elle est chargée de veiller à la **protection des données personnelles** contenues dans les fichiers et traitements informatiques ou papiers, aussi bien publics que privés.

Ainsi, elle est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

La CNIL est une **autorité administrative indépendante** (AAI), c'est-à-dire un organisme public qui agit au nom de l'État, sans être placé sous l'autorité du gouvernement ou d'un ministre.

Elle est composée de 18 membres élus ou nommés et s'appuie sur des services.

Elle a un rôle d'alerte, de conseil et d'information vers tous les publics mais dispose également d'un pouvoir de contrôle et de sanction.

Ressource 10 : Les missions de la CNIL

https://www.cnil.fr/fr/les-missions-de-la-cnil

5 – A partir des ressources 9 et 10, énumérez les missions de la CNIL, en insistant sur son rôle par rapport au RGPD.

Ressource 11 : 2019 : année de la tolérance zéro pour la CNIL !

Par Jérôme Giusti, Avocat (31 octobre 2019)

https://www.village-justice.com/articles/2019-annee-tolerance-zero-pour-cnil,32823.html

6.1 - Dans l'article accessible par le lien (ressource 11), repérez un cas de sanction par la CNIL, pour non-conformité au RGPD.

6.2 - Résumez les faits pour ce cas.

6.3 - Quel principe du RGPD n'était pas respecté ?

DOSSIER 2 : traiter un cas d'entreprise en rédigeant une note de synthèse

Il vous est demandé dans un premier temps d'accompagner la mise en place du RGPD pour une PME, le garage Maréchal.

Après un rappel de la notion de donnée personnelle et de l'importance de protéger l'identité numérique, vous recenserez les grands principes du RGPD et vous indiquerez si selon vous le site du garage répond à ces exigences réglementaires. Vous complèterez l'annexe 1 sur les données du fichier clients ; elle est à commenter et à joindre à votre note de synthèse.

Puis vous rappellerez les missions de la CNIL en insistant sur son rôle par rapport au RGPD. Vous indiquerez à quel type de sanction le garage s'expose s'il ne respecte pas ses obligations par rapport au RGPD.

Enfin vous donnerez votre avis sur la situation du garage par rapport à la mise en œuvre du RGPD.

Il vous est demandé dans un second temps d'élargir votre analyse au cas d'une grande entreprise et d'expliquer les impacts du RGPD sur l'organisation et ses activités.

Dans cette seconde partie de votre note de synthèse vous décrirez l'organisation des services et des activités mise en place dans une grande entreprise comme IBM pour respecter la législation induite par le RGPD.

Vous avez à votre disposition :

- Les ressources notionnelles du dossier 1 et l'accès au site du garage Maréchal https://www.garage-marechal.com/
- La liste de données susceptibles d'être demandées aux clients et consignées dans le fichier de l'entreprise Maréchal (annexe 1).
- La mise en place du RGPD dans une grande entreprise, expliquée par un responsable d'IBM ; les impacts en termes d'organisation des services et des activités (annexe 2).

ANNEXE 1

Données du fichier clients

En application du principe de proportionnalité et pertinence, énoncez si les données peuvent figurer légalement dans le fichier client du garage Maréchal

Données	Oui	Non	Justification
Nom			
Prénom			
Adresse			
Code postal			
Ville			
Mobile			
Mail			
N° de sécurité sociale			
Situation de famille			
Nombre d'enfants			
Profession			
Nom de l'employeur			
Adresse de l'employeur			
Immatriculation véhicule 1			
Marque véhicule 1			
Modèle véhicule 1			
Date 1re mise en circulation véhicule 1			
Date dernier contrôle technique véhicule 1			
…			

ANNEXE 2

Du RGPD vu d'une PME… au RGPD vu d'une entreprise multinationale :

les impacts sur l'organisation et sur l'activité.

Le RGPD à l'échelle d'IBM

D'après des propos recueillis auprès de François de Préville – IBM France – juin 2020

Chez IBM qui est une entreprise multinationale, comment la mise en conformité avec le RGPD s'est-elle organisée ?

F. de Préville – Pour la mise en conformité avec le RGPD en 2018 une équipe a été mise en place au niveau mondial, relayée par des responsables nommés localement dans chaque pays, et chaque entité d'IBM.

Société américaine créée en 1911 sous le nom de Computing Tabulating Recording company (CTR) et rebaptisée en 1924 sous le nom d'IBM (International Business Machines), cette entreprise multinationale a longtemps conçu et commercialisé des matériels informatiques. Aujourd'hui l'activité d'IBM se répartit entre les matériels, les logiciels et les services informatiques.

Et maintenant existe-t-il une équipe dédiée à la mise en œuvre du RGPD ?

F. de Préville – Il existe un premier niveau de gouvernance et surveillance : le Privacy advisory committee (comité conseil sur la confidentialité/ou sur la protection des données personnelles). Puis au niveau des unités commerciales IBM sont nommés des Responsables de la sécurité des informations commerciales, et des data privacy leaders (responsables de la confidentialité des données) pour chaque pays où IBM est implantée. Enfin un correspondant est déclaré à la CNIL.

Quels sont les principaux services impactés par le RGPD ?

F. de Préville – Les services les plus impactés sont les **Ressources Humaines** qui doivent gérer les données personnelles des employés et des candidats au recrutement, mais également les services **Achats** qui conservent les données personnelles des fournisseurs, les services **Marketing** qui stockent les données personnelles des clients, prospects et partenaires commerciaux, les services de **Ventes** et les **services techniques** au contact des clients, et enfin les **services juridiques** qui gèrent tous les contrats.

Pouvez-vous nous donner des exemples de mesures concrètes mises en place pour assurer la conformité d'IBM au RGPD ?

F. de Préville – La mise en place des instances citées plus haut s'est accompagnée de la création de différents **supports** comme par exemple :

- Des ressources d'auto-assistance :

  - Base de connaissances sur la confidentialité et la protection des données
  - FAQs (liste de réponses aux questions les plus fréquemment posées) sur la confidentialité et la protection des données
  - Conseils spécifiques au RGPD

- Un service d'assistance sur la confidentialité des données auquel chaque « IBMer" peut s'adresser pour obtenir de l'aide sur les problèmes de confidentialité et de protection des données.

Chaque IBMer qui détient un fichier de données personnelles doit faire le nécessaire pour gérer ces informations conformément aux exigences et aux valeurs d'IBM. De nombreux employés ont donc bénéficié de **formations,** et différents **programmes** ont été créés afin de :

- permettre l'automatisation et l'évolutivité des applications backend et des processus métier d'IBM afin de mieux répondre à la complexité réglementaire croissante et aux demandes toujours plus nombreuses du marché pour une gestion responsable des données ;
- décrire les mesures que les équipes de produits et d'offres IBM doivent mettre en œuvre pour garantir que les solutions qu'elles mettent sur le marché respectent les normes applicables de l'industrie et les réglementations gouvernementales en matière de cybersécurité et de confidentialité ;
- traiter au plus vite les incidents impliquant la perte ou la compromission d'informations IBM ou contrôlées / détenues par le client, ce qui peut avoir de graves conséquences négatives pour IBM et ses clients ;
- indiquer comment gérer les demandes de droits des personnes concernées d'IBM et de tiers ;
- évaluer les processus commerciaux, les applications et les autres initiatives qui traitent les informations personnelles (IP) contrôlées par IBM, par rapport à leur conformité aux lois sur la confidentialité et aux politiques d'entreprise applicables.

Certains **processus** ont dû être modifiés ou créés, de nouveaux **rôles** sont apparus, il a fallu déployer de **nouveaux outils et technologies**.

Les **contrats** ont dû être complétés de façon à les rendre compatibles RGPD.

Quelles sont les procédures à respecter pour chaque entité ?

F. de Préville – Il faut par exemple rédiger et tenir à jour toute la documentation sur les traitements de données personnelles (registre des traitements…), stocker des « évidences » (preuves) qui permettent de démontrer que les règles du RGPD sont respectées…, rédiger et tenir à jour les procédures sur l'information des personnes…

Au-delà des contraintes imposées par le RGPD, sa mise en œuvre permet-elle une meilleure gestion des données personnelles ?

F. de Préville – Le RGPD a contribué à transformer la gestion des problèmes de confidentialité, des droits des données et des violations de la sécurité en pratiques commerciales standards. La réputation de longue date d'IBM en tant que gestionnaire responsable de la technologie et des données nous positionne parfaitement en tant que partenaire de confiance pour les clients confrontés à un paysage réglementaire de plus en plus complexe et difficile. La réputation d'IBM en matière de protection des données est très forte. Depuis plus d'un siècle, IBM a gagné la confiance de ses clients en gérant de manière responsable leurs données les plus précieuses, et nous avons travaillé pour gagner la confiance de la société en introduisant de nouvelles technologies puissantes dans le monde de manière responsable et avec un objectif clair.

Enfin, le RGPD a-t-il occasionné d'autres opportunités pour IBM ?

Au-delà du renforcement de la confiance avec les clients que nous venons d'aborder, IBM a pu développer la commercialisation de ses solutions de chiffrement qui permettent de sécuriser les données. L'entreprise a pu également étendre son offre de services en proposant un accompagnement aux entreprises sur la sécurisation et la protection des données.

Plus qu'une contrainte réglementaire, c'est la confiance et le respect des clients et des personnes que le management d'IBM monde, Europe et France a mis au centre du déploiement du RGPD pour responsabiliser l'ensemble des personnels pour porter et afficher la valeur de l'éthique comme partie intégrante de la promesse de l'entreprise.

D’une menace liée à la sanction en cas de non-respect du RGPD, très dissuasive et déclenchée par signalement des clients, l’entreprise en a fait à la fois un objet d’engagement auprès de ses clients dans lequel chaque salarié d’IBM est lui-même engagé.

DOSSIER 3 : rédiger l’essentiel de ce qu’il vous faut retenir du travail effectué

Vous souhaitez garder la trace de ce qu’il faut retenir sur le travail que vous venez de réaliser.

À ce titre, vous rédigez un court mémo que vous conserverez pour vous en respectant le plan ci-dessous :

- *Définition des données personnelles et de l’identité numérique*
- *La nécessaire adaptation du droit*
- *Les grands principes du RGPD*
- *Le rôle de la CNIL*
- *Les impacts en termes d’organisation pour les entreprises selon les actions à mettre en place concernant la protection des personnes et des données*
- *Les conséquences juridiques de ces choix et les conséquences juridiques en cas de non-respect du cadre légal*