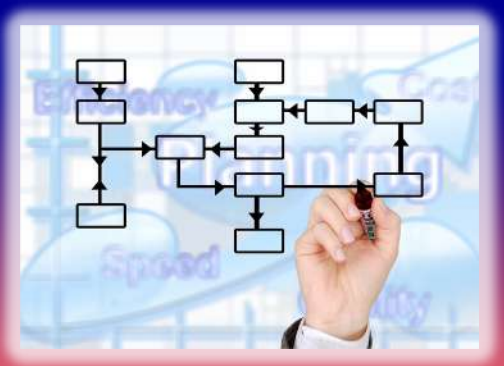
IFCE
MS2 Mngt projet Marketing

RGPD et Marketing

1

1

IFCE
MS2 Mngt projet Marketing



SOMMAIRE

OBJECTIF

CONTENU

2

2

OBJECTIF

Prendre en compte le RGPD au sein de l'entreprise et notamment dans le domaine Marketing

3

3

CONTENU

Expliquer le fondement RGPD

Comprendre les principes

Présentation des outils

Sensibilisation à la protection du patrimoine de l'entreprise

4

4

IFCE
MS2 Mngt projet Marketing

1ère partie
RGPD – pour qui, pourquoi?

- CADRE HISTORIQUE
- RGPD – KEZACO?
- LE FOND
- UNE HISTOIRE DE DONNÉES

5

5

CADRE HISTORIQUE

1974: Première prise de conscience en France de l'importance de protéger les données.

-projet "**SAFARI**" (système automatisé pour les fichiers administratifs et le répertoire des individus, créé par l'Insee en 1973),

L'idée du gouvernement: **pouvoir identifier chaque citoyen grâce à l'interconnexion de tous les fichiers de l'administration.**

6

6

CADRE HISTORIQUE

1978: création de la CNIL et 1ère loi.

-Mission= **accompagner** les évolutions informatiques, en veillant à ce que cela reste un progrès pour les citoyens, sans atteinte à leur liberté ni à leur vie privée.

7

7

CADRE HISTORIQUE

1995: directive européenne

- Principe: les données personnelles ne doivent pas être soumises à un traitement automatisé, sauf si celui-ci remplit les exigences posées par trois principes: **proportionnalité, transparence, et finalité légitime**.

- Le cadre juridique général de la loi de 1978 est repris.

8

8

CADRE HISTORIQUE

2004: directive européenne

- Si la loi n° 78-17 du 6 janvier 1978 parlait d'"informations nominatives", la loi n° 2004-801 du 6 août 2004 parle dorénavant de **"données à caractère personnel"**

9

9

CADRE HISTORIQUE

2016: **RGPD (Règlement Général pour la Protection des Données)**

- Travail effectué par le G29 (groupe de travail européen sur la protection des données).
- Adopté par le parlement européen le 14 avril 2016, et devient obligatoire le 25 mai 2018.

10

10

RGPD - KEZACO

- 88 pages de texte
- 99 articles

- Toute entité, traitant des données d'ordre personnel devra se soumettre à ce règlement.

11

11

RGPD – LE FOND

<u>But:</u> **harmoniser la protection des libertés et des droits fondamentaux des personnes physiques** en ce qui concerne **les activités de traitement** et à assurer le libre flux des données à **caractère personnel** entre les états membres.

12

12

- Transformation de la typologie de données

13

13

- **Transformation de la typologie de données**.

Avant:

Nom –prénom
Adresse
Téléphone
Code client

Maintenant:

Nom –prénom
Adresse
Téléphone
Code client
Pseudonyme
IP
Adresse MAC
Données de traçage
Données partagées
Réseaux sociaux
…

14

14

- Transformation de la typologie de données
- Transformation de la quantité de données

15

15

- **Transformation de la quantité de données**

16

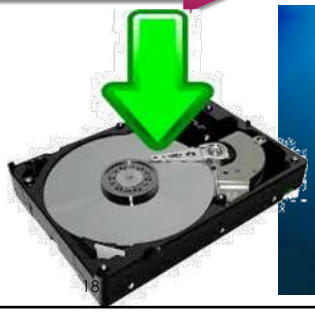
16

- Transformation de la typologie de données
- Transformation de la quantité de données
- Transformation du flux de transfert de données

17

17

- **Transformation du flux de transfert de données**



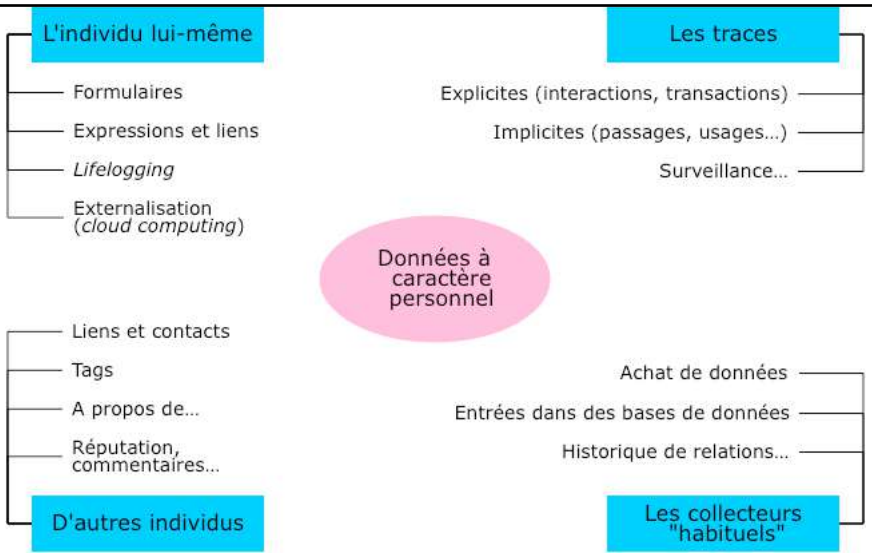
18

18

- Transformation de la typologie de données
- Transformation de la quantité de données
- Transformation du flux de transfert de données
- Transformation de l'utilisation des données

19

19



- **Transformation de l'utilisation des données**

20

20

21

21

Comment faire face à une utilisation potentiellement préjudiciable dans cet environnement en mouvance perpétuelle?

22

22

RGPD – UNE HISTOIRE DE DONNÉES

23

23

Une donnée personnelle (ou donnée à caractère personnel) est une information qui permet

>d'identifier une personne physique, directement ou indirectement.

24

24

Il peut s'agir :

d'un nom,
d'une photographie,
d'une adresse IP,
d'un numéro de téléphone,
d'un identifiant de connexion informatique,
d'une adresse postale,
d'une empreinte,
d'un enregistrement vocal,
d'un numéro de sécurité sociale,
d'un mail,
De coordonnées bancaires
etc…

25

25

Données internes

Les données concernant les collaborateurs et les intervenants de l'entreprise, utilisées au sein de la structure constituent les données internes.

26

26

Données externes

Les données concernant les clients, prospects, fournisseurs, les personnes physiques comme apporteurs d'affaires, points de contact externes, représentent les données externes.

27

27

Accès aux prestataires

Les organismes qui traitent des données personnelles pour le compte d'un autre organisme (**les sous-traitants** comme, par exemple, des prestataires de services informatiques ou des agences de marketing ou de communication qui **traitent des données personnelles pour le compte de leurs clients**) doivent tenir **un registre de leurs activités** de sous-traitant impliquant le traitement de données.

28

28

Données sensibles

Elles touchent à des informations qui peuvent donner lieu à de **la discrimination ou des préjugés** :

Une opinion politique,
une sensibilité religieuse,
un engagement syndical,
une appartenance ethnique,
une orientation sexuelle,
une situation médicale,
des idées philosophiques.

Elles ont un cadre particulier, qui interdit toute collecte préalable sans consentement écrit, clair et explicite, et pour des cas précis, validés par la Cnil et dont l'intérêt public est avéré.

29

29

IFCE
MS2 Mngt projet Marketing

2ème partie
RGPD – Les étapes de la mise en place

- LE DATA PROTECTION OFFICER
- PRISE DE HAUTEUR
- REGISTRE(**S**) DE TRAITEMENT
- ANALYSE D'IMPACT
- SENSIBILISATION

30

30

Le DPO ou DPD (Délégué à la Protection des Données)

Le DPO (ou data protection officer) est le **« Chef d'orchestre »** de la conformité en matière de protection des données au sein de son organisme

31

31

Concernant les TPE - PME

Les TPE-PME peuvent nommer une personne en interne (poste technique, juridique, …) ou en externe (DPO, avocat, consultant, …) qui se chargera de maintenir le registre de traitement à jour, de s'assurer de l'application de la RGPD et de coopérer avec la CNIL si nécessaire > ***ACCOUNTABILITY***

Le Chef d'entreprise est le seul responsable du traitement des données à caractère personnel et de l'application de la RGPD au regard de sa position de direction.

32

32

Rôle du DPO ou du Délégué ou du responsable des données

- **informer** et conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;
- **contrôler** le respect du règlement et du droit national en matière de protection des données ;
- **conseiller** l'organisme sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution ;
- **coopérer** avec l'autorité de contrôle et d'être le point de contact de celle-ci.

33

33

Organiser la fonction du DPO

les missions suivantes sont confiées au « futur » délégué :

- **réaliser l'inventaire** des traitements de données personnelles mis en œuvre ;
- **évaluer** ses pratiques et mettre en place des procédures (audits, privacy by design, notification des violations de données, gestion des réclamations et des plaintes, etc.) ;
- **identifier les risques** associés aux opérations de traitement ;
- **établir une politique** de protection des données personnelles ;
- **sensibiliser** les opérationnels et la direction sur les nouvelles obligations.

34

34

La prise de hauteur - État des lieux

- Demande de consentement
- Mentions légales
- Transparence
- Droit à l'oubli
- Accès aux données
- Durée de conservation

39

39

État des lieux

Quelles sont les pratiques internes concernées par le dispositif RGPD?

- CRM – ERP
- Emailing
- Site web
- CGV
- Newsletter
- Base de données du personnel
- **Et toute activité donnant lieu à l'utilisation et au traitement des données à caractère personnel**

40

40

Licéité de traitement

C'est la base légale – Article 6-1
Un traitement est licite et peut être mis en œuvre si l'une des 6 conditions suivante est remplie:

1. La personne concernée **a consenti** au traitement de ses données à caractère personnel
2. Le traitement est nécessaire à **l'exécution d'un contrat**
3. Le traitement est nécessaire au **respect d'une obligation légale**
4. Le traitement est nécessaire à la **sauvegarde des intérêts vitaux de la personne concernée**
5. Le traitement est nécessaire à l'exécution **d'une mission d'intérêt publique** ou relevant de l'exercice de l'autorité publique
6. Le traitement est nécessaire aux fins des **intérêts légitimes poursuivis par le responsable de traitement**. (vidéosurveillance par exemple)

41

41

Le consentement

B2C
Obtenir de la part de l'intéressé, le consentement d'utiliser ses données à caractère personnel en indiquant les finalités pour lesquelles elles sont utilisées.

Proposer une durée de conservation

Garder une trace du consentement

B2B

Lors d'un contact mail, assurer au destinataire la possibilité de prendre connaissance de la finalité d'utilisation des données

Possibilité de faire de l'Opt-Out

42

42

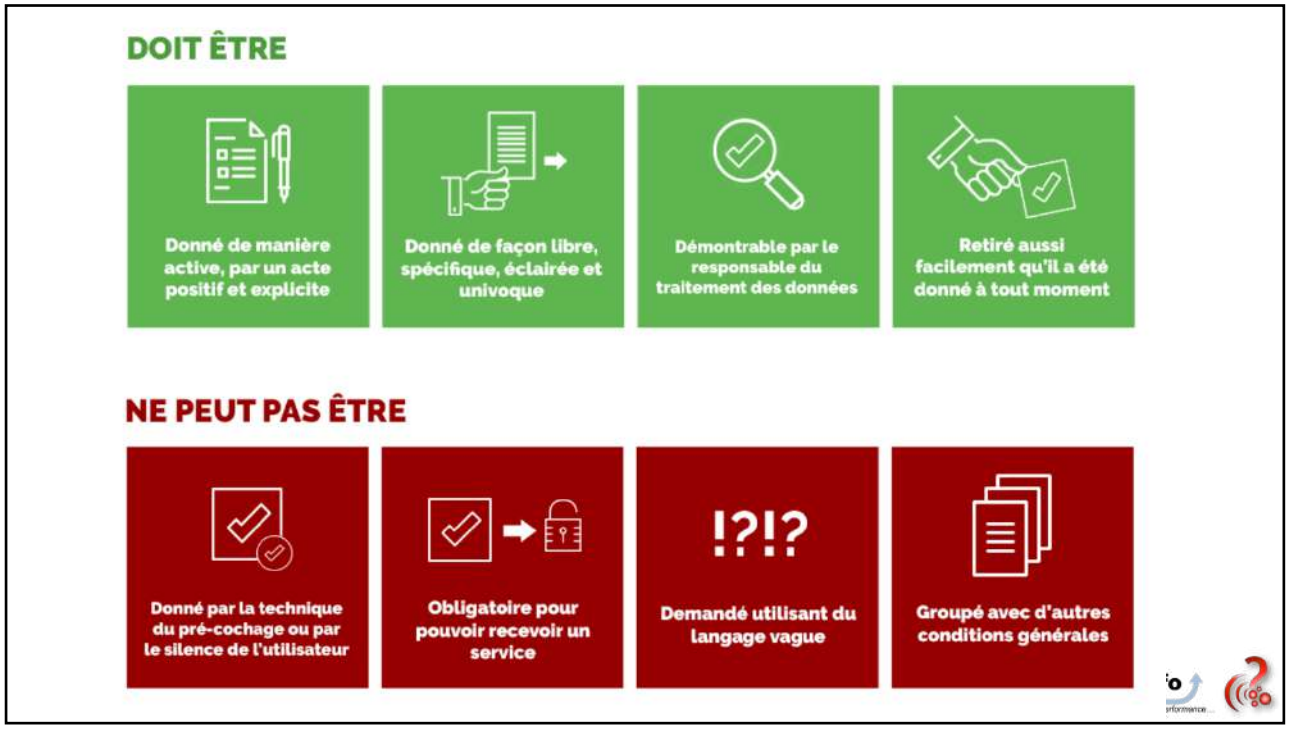
Le consentement

- Il doit être **libre** (ni contraint, ni influencé),
- **spécifique** (correspondre à un seul traitement pour une finalité déterminée),
- **éclairé** (précédé d'informations communiquées à la personne concernée)
- **univoque** (sans ambiguïté sur son expression).

Ces quatre conditions doivent être cumulées pour que ce consentement soit valablement recueilli.

43

43



44

Quand est ce que le consentement de la personne dont des données sont enregistrées dans un fichier n'est pas nécessaire :

- **Pour l'exécution d'un contrat** (Ex : contrat de vente, de location, de travail, etc.) ou de mesures précontractuelles (ex : un devis, des pourparlers, etc.).
- **Parce qu'un texte légal rend obligatoire certains fichiers** (ex : le recensement de la population par l'INSEE, le registre unique du personnel, etc.).
- **Pour l'exécution d'une mission d'intérêt public ou relevant de l'autorité publique** (ex : constitution de fichiers de police, de l'administration fiscale, etc.).

45

45

Quand est ce que le consentement de la personne dont des données sont enregistrées dans un fichier n'est pas nécessaire :

- **Pour sauvegarder les intérêts vitaux d'une personne** (ex : en cas d'épidémie, dans les situations de catastrophe naturelle ou d'origine humaine, etc.).
- **Pour un intérêt légitime** (ex : la prévention de la fraude, les transferts au sein d'un groupe, la sécurité des réseaux, etc.) sauf si les intérêts ou les libertés fondamentales de la personne concernée prévalent.

A savoir : Le recueil du consentement des personnes ne dispense pas de les informer de leurs droits (articles 13 et 14 du RGPD).

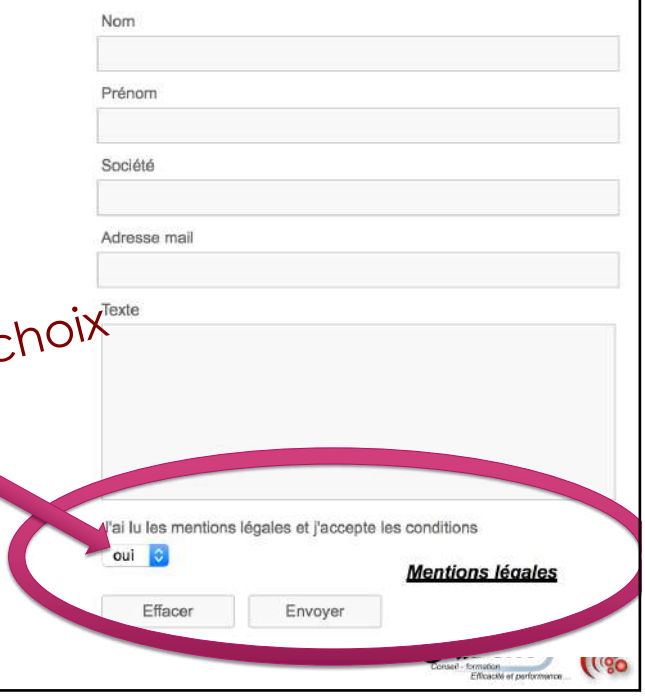
46

46

Ok ou Pas?

NON

- Case pré-cochée
- Message non clair
- Pas de possibilité de choix



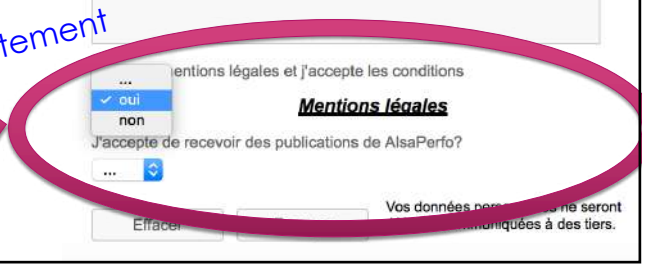
47

Ok ou Pas?

Pour répondre à l'intéressé, ces données sont simplement facultatives et ne doivent pas être obligatoires

OUI

- Choix de l'intéressé
- Message additionnel clair
- Pour chaque traitement, un consentement



48

48

Le consentement (on garde une trace)

Nom
Dupont
Prénom
Albert
Société
ConsultStrat
Adresse mail
albert.dupont@consultstrat.com
Texte
Ceci est un message de démonstration.
Les noms et fonctions sont fictifs

J'ai lu les mentions légales et j'accepte les conditions
oui
Mentions légales

J'accepte de recevoir des publications de AlsaPerfo?
non

Effacer | Envoyer

Vos données personnelles ne seront JAMAIS communiquées à des tiers.

De Moi <contact@alsaperfo.fr>
Sujet **AlsaPerfo website**
Réponse à albert.dupont@consultstrat.com
Pour Moi <contact@alsaperfo.fr>
Date Sat, 25 Aug 2018 08:22:28 -0000
Identifiant du message <mailbox-10838-1535185349-512073@mailrelay1-2.ispfr.net>
Received from mx3.ispfr.net by clmail-mxmol4.intra (Dovecot) with LMTP id SZk0

Nom
Dupont

Prénom
Albert

Société
ConsultStrat

Adresse mail
albert.dupont@consultstrat.com

Ceci est un message de démonstration.
Les noms et fonctions sont fictifs

J'ai lu les mentions légales et j'accepte les conditions
oui

J'accepte de recevoir des publications de AlsaPerfo?
non

49

49

Les mentions légales sur le net.

Ce site a été élaboré par André SCHWENK, dirigeant de SCHWENK ANDRE DOMINIQUE dont le siège social se situe au 110 Grand'Rue 67110 Gundershoffen - FRANCE.
Siret: 818 078891 00012
Numéro de déclaration d'activité de prestataire de formation : 44670616467 délivré par le préfet du Bas-Rhin
Tél: +33620834416.

Le site est hébergé par NUXIT s.a.r.l.
LIR
400 avenue Roumanille BP 309
06906 Sophia Antipolis Cedex
FRANCE
phone:+33899563600

Les informations collectées répondent au Règlement Général de la Protection des Données en vigueur.
Ainsi, les informations et données personnelles ne sont collectées qu'après consentement de l'intéressé(é) et sauvegardées durant la période nécessaire à la fourniture de la réponse à la question posée.

En cochant la case de consentement obligatoire avant soumission de chaque formulaire du site web www.alsaperfo.fr vous autorisez explicitement le stockage et le traitement de vos données dans le but de vous faire connaître nos services. Vous autorisez :
- Un conseiller de l'entreprise André Dominique SCHWENK à vous contacter pour toute relation commerciale.
- Le service Marketing à vous communiquer des informations personnalisées sur nos services.

Vous ne souhaitez pas donner votre consentement ? Appelez-nous directement au +33 6 20 83 44 16. Nous répondrons ainsi à vos questions par téléphone.

Nous utilisons des cookies de la part de Google Analytics. Les données et statistiques que nous collectons au moyen de ces cookies sont utilisées dans le seul et unique but d'améliorer la qualité de nos services.
Google Analytics est utilisé de façon anonyme afin d'améliorer l'expérience utilisateur sur notre site web et vous offrir une navigation intuitive.
Les données ne sont pas utilisées à des fins commerciales ou de profilage. Les données ne sont pas cédées à des tiers sous quelque forme que ce soit.
Vous pouvez prendre connaissance des données vous concernant sur demande explicite et écrite à l'adresse suivante contact@alsaperfo.fr
La demande sera gérée dans les plus brefs délais et dans tous les cas en moins d'un mois.
Vous pouvez ainsi demander la modification et la suppression suivant le principe du droit à l'oubli, et toute demande

50

50

Que dit la loi?

https://www.service-public.fr/professionnels-entreprises/vosdroits/F31228

51

Mentions relatives à l'utilisation de données personnelles
Les sites qui utilisent des données personnelles doivent obligatoires mentionner les informations suivantes :

•Coordonnées du délégué à la protection des données (DPO ou DPD) de l'organisme, s'il a été désigné, ou d'un point de contact sur les questions de protection des données personnelles
•Finalité poursuivie par le traitement auquel les données sont destinées
•Caractère obligatoire ou facultatif des réponses et conséquences éventuelles à l'égard de l'internaute d'un défaut de réponse
•Destinataires ou catégories de destinataires des données
•Droits d'opposition, d'interrogation, d'accès et de rectification
•Au besoin, les transferts de données à caractère personnel envisagés à destination d'un État n'appartenant pas à l'Union européenne
•Base juridique du traitement de données (c'est-à-dire ce qui autorise légalement le traitement : il peut s'agir du consentement des personnes concernées, du respect d'une obligation prévue par un texte, de l'exécution d'un contrat notamment)
•Mention du droit d'introduire une réclamation (plainte) auprès de la Cnil

52

Attention :
l'absence d'une information obligatoire est punie d'une amende de 1 500 €.
Tout traitement informatique non consenti des données recueillies est puni de 5 ans d'emprisonnement et de 300 000 € d'amende.

53

La question des cookies. (1)

Etape 1 : Informer sur les cookies utilisés et leur finalité

l'internaute qui se rend sur le site d'un éditeur (page d'accueil ou page secondaire du site) doit être informé, par l'apparition **d'un bandeau** :

- des finalités précises des cookies utilisés ;
- de la possibilité de s'opposer à ces cookies et de changer les paramètres en cliquant sur un lien présent dans le bandeau ;
- du fait que la **poursuite de sa navigation vaut accord au dépôt de cookies sur son terminal**.

54

54

La question des cookies. (2)

Etape 2 : Une page "En savoir plus " permettant à l'utilisateur de paramétrer les cookies.

informer de manière claire et concise l'usager sur ce qu'est un cookie et lui offrir la possibilité d'exprimer son choix, après la description de la finalité de chaque famille de cookies.

Dans la mesure où le consentement ne doit pas être ambigu, **ce bandeau ne doit pas disparaître tant que la personne n'a pas poursuivi sa navigation**.

Le fait de visiter la page "en savoir plus" ne vaut pas consentement au dépôt de cookies.

55

55

Mentions relatives à l'utilisation de cookies

Un cookie est un petit fichier informatique, un traceur. Il permet d'analyser le comportement des usagers lors de la visite d'un site internet, de la lecture d'un courrier électronique, de l'installation ou de l'utilisation d'un logiciel ou d'une application mobile.

Les éditeurs de sites ou d'applications qui utilisent des cookies doivent :
•informer les internautes de la finalité des cookies,
•obtenir leur consentement,
•fournir aux internautes un moyen de les refuser.

La durée de validité du consentement donné dans ce cadre est de 13 mois maximum.

56

ATTENTION

La délibération n°2019-093 du 4 juillet 2019 de la CNIL, publiée le 18 juillet au Journal Officiel, signe la **mort du soft opt-in** et ouvre la voie à un **consentement actif des utilisateurs sur les cookies et les traceurs.**
Pourquoi un tel changement ? Le RGPD est passé par là et les règles de la CNIL datant de 2013 étaient devenues caduques.

57

58

www.alsaperfo.fr
Les plus visités
Débuter avec Firefox
André SCHWENK
Conseil - Formation
Gestion de l'information
@lsaPerfo
Conseil - formation
Efficacité et performance...
Chercher
Accueil
Qui est alsaperfo
Infos net
Blog
Contact
Shares
Processus de recherche et de veille
Gestion de l'information
Gestion de projets et cartes mentales
SUN TZU. L'Art de la guerre (VIème siècle av. J.-C.)
Puis on a eu cela
Ce site Web utilise des cookies
Les cookies nous permettent de personnaliser le contenu et les annonces, d'offrir des fonctionnalités relatives aux médias sociaux et d'analyser notre trafic. Nous partageons également des informations sur l'utilisation de notre site avec nos partenaires de médias sociaux, de publicité et d'analyse, qui peuvent combiner celles-ci avec d'autres informations que vous leur avez fournies ou qu'ils ont collectées lors de votre utilisation de leurs services. Vous consentez à nos cookies si vous continuez à utiliser notre site Web.
Nécessaires
Préférences
Statistiques
Marketing
Afficher les détails
OK
MASTER CLASS

59

https://www.alsaperfo.fr
Pas en cours de synchronisation
@lsaPerfo
Conseil - formation
Accueil
Actuellement
c'est ceci
SUN TZU. L'Art de la guerre (VIème siècle av. J.-C.)
Pour vous, TPE et PME
Ce site Web utilise des cookies
Les cookies nous permettent de personnaliser le contenu et les annonces, d'offrir des fonctionnalités relatives aux médias sociaux et d'analyser notre trafic. Nous partageons également des informations sur l'utilisation de notre site avec nos partenaires de médias sociaux, de publicité et d'analyse, qui peuvent combiner celles-ci avec d'autres informations que vous leur avez fournies ou qu'ils ont collectées lors de votre utilisation de leurs services. Vous consentez à nos cookies si vous continuez à utiliser notre site Web.
Autoriser tous les cookies
Autoriser la sélection
Utiliser uniquement les cookies nécessaires
Nécessaires
Préférences
Statistiques
Marketing
Afficher les détails

60

Exemple des explications de gestion des cookies proposé dans la politique de confidentialité sur le site Internet.

54

Déclaration relative aux cookies mise à jour le 03/03/2020 par Cookiebot:

Nécessaires (3)

Les cookies nécessaires contribuent à rendre un site Web utilisable en activant des fonctions de base comme la navigation de page et l'accès aux zones sécurisées du site Web. Le site Web ne peut pas fonctionner correctement sans ces cookies.

Nom	Fournisseur	Finalité	Expiration	Type
CookieConsent	Cookiebot	Stocke l'autorisation d'utilisation de cookies pour le domaine actuel par l'utilisateur	1 année	HTTP Cookie
local_storage_support_test	Twitter	Le cookie est utilisé dans le contexte de la fonction de stockage local dans le navigateur. Cette fonction permet au site Web de se charger plus rapidement en pré-chargeant certaines procédures.	Persistent	HTML Local Storage
PHPNET-MNO	alsaperfo.fr	Enregistre quel groupe de serveurs sert le visiteur. Ceci est utilisé dans le contexte de l'équilibrage de charge afin d'optimiser l'expérience utilisateur.	Session	HTTP Cookie

61

Cookie banner Cnil

https://www.cnil.fr/fr/exemple-de-bandeau-cookie

Modèle de bandeau d'information préalable

Voici un modèle à utiliser pour des cookies publicitaires et de mesure d'audience. Il doit être adapté en fonction de la finalité des cookies utilisés.

En poursuivant votre navigation sur ce site, vous acceptez l'utilisation de ***[Cookies ou autres traceurs]*** *pour vous proposer* ***[Par exemple, des publicités ciblées adaptés à vos centres d'intérêts]*** *et* ***[Par exemple, réaliser des statistiques de visites]****.*

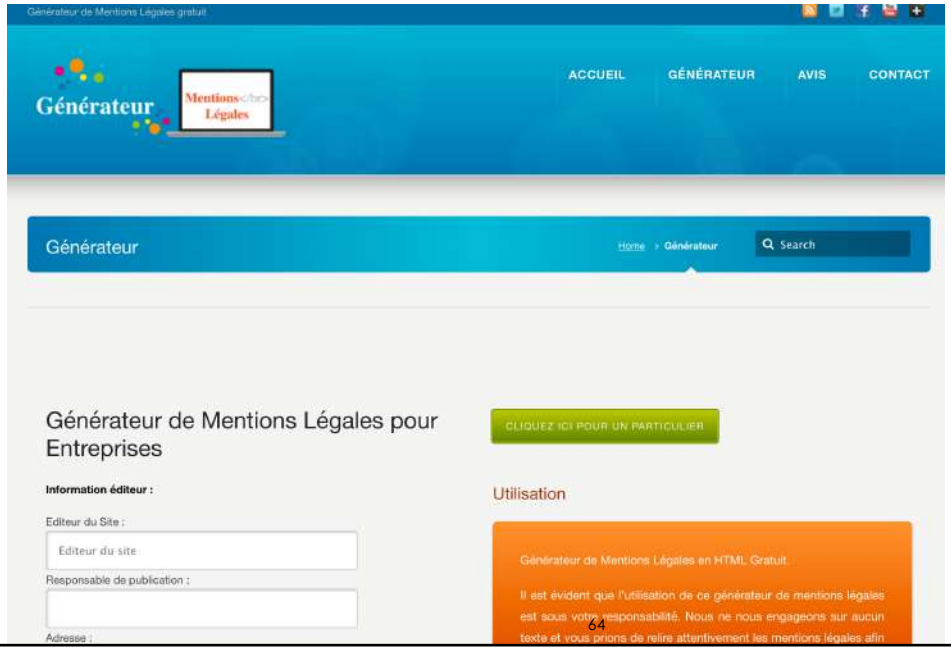
Pour en savoir plus et paramétrer les traceurs

62

62

63

https://generateur-de-mentions-legales.com/generateur/



64

64

La transparence

Pourquoi? Parce qu'elle permet à l'intéressé:

- de **connaître** la raison de la collecte des différentes données les concernant ;
- de **comprendre** le traitement qui sera fait de leurs données ;
- d'**assurer la maîtrise** de leurs données, en facilitant l'exercice de leurs droits.

65

65

La transparence
Dans quel cas informer?(1)

Collecte directe

- formulaire,
- achat en ligne,
- souscription d'un contrat,
- ouverture d'un compte bancaire
- vidéosurveillance,
- analyse de la navigation sur Internet,
- Géolocalisation,
- wifi analytics/tracking

66

66

La transparence
Dans quel cas informer?(2)

Collecte indirecte

- données récupérées auprès de partenaires commerciaux,
- de data brokers,
- de sources accessibles au public,
- d'autres personnes

67

67

La transparence
C'est aussi pour les collaborateurs

- Utilisation de leur nom, prénom, parfois numéro de téléphone perso.
- Les données pour la gestion des paies.
- Les données de localisation.
- Droit à l'image ou publications
- …

68

68

Accès aux données

Une personne ayant donné son consentement doit pouvoir avoir **avoir accès à ses données, les modifier, les supprimer.**

Délai de réponse à une demande d'accès aux données à caractère personnel: **un mois** (extensible à 3 suivant la complexité et le nombre de demandes et après justification auprès de l'intéressé dans un délai d'un mois)

69

69

Le droit à l'oubli

Ainsi, toute personne dont les données sont conservées dans une entité, de par son information de la structure conservant ces données, peut avoir accès à ces éléments et ainsi faire valoir le droit à l'oubli, en d'autres termes ici, le droit à l'effacement des données à caractère personnel la concernant.

70

70

La durée de conservation

Le nouveau règlement impose de limiter dans le temps la conservation de données à caractère personnel et d'en informer les intéressés (transparence).

Exemple: données concernant les prospects < 3 ans
Curriculum vitae < 2 ans,…

71

71

La durée de conservation

Le principe veut que la **durée de conservation des données ne puisse excéder la durée de la finalité**.

Une fois que l'objectif poursuivi par la collecte des données est atteint, il n'y a plus lieu de les conserver et **elles doivent être supprimées**.

72

72

La durée de conservation vs durée d'archivage

La durée de conservation se distingue de la durée d'archivage.

Durée de conservation = période d'utilisation des données. Cette période est déterminée par la finalité.

La durée d'archivage est quant à elle nécessairement supérieure à cette finalité.

73

73

Le(s) Registre(s) de Traitement

- Pour qui?
- L'outil
- Le but
- La mise à jour

74

74

Au-delà de la réponse à l'obligation prévue par l'article 30 du RGPD, le registre est **un outil de pilotage et de démonstration de votre conformité au RGPD**

75

75

Pour qui?

L'obligation de tenir un registre des traitements concerne tous les organismes, publics comme privés et quelle que soit leur taille, dès lors qu'ils traitent des données personnelles.

76

76

Pour les sous-traitants

Les organismes assurant la sous-traitance, c'est à dire, ayant eu délégation pour traiter des données à caractère personnel depuis un organisme client, doivent, **EN PLUS** de leur registre de traitement, tenir un **registre de sous-traitant**

77

77

L'outil

Une première page du registre recense les informations communes à toutes vos activités de traitement.

- **Les coordonnées de votre organisme** (ou de son représentant sur le territoire européen si votre organisme n'est pas établi dans l'Union européenne)
- **Les coordonnées du délégué à la protection des données** (DPO) si vous en disposez
- **La liste des activités** de votre organisme impliquant le traitement de données personnelles.

Pour chaque activité recensée, vous devrez créer et tenir à jour une fiche de registre.

78

78

L'outil

Registre des activités de traitement de [Nom de l'organisme]

Coordonnées du responsable de l'organisme *(responsable de traitement ou son représentant si le responsable est situé en dehors de l'UE)*	*Ex : NOM prénom du responsable légal* *Adresse* *CP VILLE* *Téléphone* *Adresse de messagerie*
Nom et coordonnées du délégué à la protection des données *(si vous avez désigné un DPO)*	*Ex : NOM prénom du DPO* *Société (si DPO externe)* *Adresse* *CP VILLE* *Téléphone* *Adresse de messagerie*

79

79

Comment le constituer? (1)

Rassembler les informations disponibles

Identifier et rencontrer les responsables opérationnels des différents services susceptibles de traiter des données personnelles.

Si l'organisme dispose d'un site internet, l'analyser et identifier les données collectées dans les formulaires en ligne (questionnaire, formulaire de contact, création d'un compte, etc.), les mentions d'information «protection des données », l'utilisation de cookies, etc.

80

80

Comment le constituer? (2)

Lister dans un tableau de suivi les différentes activités de l'organisme nécessitant le traitement de données personnelles.

Les traitements de données doivent être identifiés par finalité et non par logiciel utilisé, car un même logiciel peut être utilisé pour différents traitements et inversement.

Sur la base des informations collectées lors des entretiens, remplir une fiche de registre par activité.

81

81

Activités	Désignation des activités (exemples)
Activité 1	*Gestion de la paie*
Activité 2	*Gestion des prospects*
Activité 3	*Gestion des fournisseurs*
Activité 4	*Vente en ligne*
Activité 5	*Sécurisation des locaux*
Activité 6	…

82

82

Activité	Gestion de la paie
NR	1
Activité	Gestion de la paie
Service traitant	Comptabilité
Nom du responsable du traitement	Mr Durand
Application ou logiciel	Excel
Objectif	Assurer le paiement des salaires des collaborateurs au regard du contrat de travail
Catégorie de personnes concernées	Salariés
Données collectées	Nom Prénom Adresse Mail Téléphone Coordonnées bancaires
Données sensibles traitées?	OUI (coordonnées bancaires)
Durée de conservation	Durée du contrat et maximum 3 ans au delà de la relation contractuelle
Destinataires internes	Comptabilité Ressources humaines Direction générale
Destinataires externes	Organisme payeur par autorisation de prélèvement sur le compte entreprise
Sous traitants	Sans objet
Transfert des données hors UE?	NON
Contrôle d'accès des utilisateurs	Login et mot de passe personnel Accès restreint à la base de données concernée aux personnels de la comptabilité (mise en place par le service informatique)
Mesures de traçabilité	Enregistrement automatique des ouvertures et modifications de fichier
Mesures de protection des logiciels	Antivirus de marque XXX mis à jour quotidiennement Supervision par le service informatique
Sauvegardes des données	Sauvegarde des données sur serveur central avec sauvegarde journalière et accès sécurisé
Chiffrement des données	Chiffrement de dossier réalisé via VeraCrypt
Contrôle des sous traitants	Sans objet
Autres mesures	
Risques	Divulgation accidentelle de données Suppression ou effacement accidentel ou volontaire des données personnelles Modification volontaire des donnée
Impact	3
Probabilité	2 84
Importance	6

84

Le but de ce registre

- Faire le ménage et tenir à jour sa base de données
- Quel type de données possède-t-on?
- En avons nous besoin? (**minimisation**)
- Établir les responsabilités quant à leur utilisation
- Encadrer l'utilisation
- Savoir qui a accès aux données (**sécurisation**)
- Connaître le cycle de vie de la donnée

Le registre n'est pas figé!!!

85

85

La mise à jour

Le registre doit être mise à jour régulièrement au gré des évolutions fonctionnelles et techniques des traitements de données.

En pratique, toute modification apportée aux conditions de mise en œuvre de chaque traitement inscrit au registre (nouvelle typologie de données collectée, allongement de la durée de conservation, nouveau destinataire du traitement, etc.) doit être portée au registre.

86

86

A qui le communiquer?

le registre est un document interne et évolutif, qui doit avant tout aider l'organisme à piloter sa conformité.

Le registre doit toutefois pouvoir être communiqué à la CNIL lorsqu'elle le demande. Elle pourra en particulier l'utiliser dans le cadre de sa mission de contrôle des traitements de données.
C'est le principe de **l'accountability**

87

87

Outils pour le registre de traitement des données

REGISTRE DE TRAITEMENT PROPOSÉ PAR LA CNIL

88

88

Registre de traitement de la CNIL

	Fiche de registre		ref-000			
Description du traitement						
Nom / sigle						
N° / REF	ref-000					
Date de création						
Mise à jour						
Acteurs	Nom	Adresse	CP	Ville	Pays	Tel
Responsable du traitement						
Délégué à la protection des données						
Représentant						
Responsable(s) conjoint(s)						
Finalité(s) du traitement effectué						
Finalité principale						
Sous-finalité 1						
Sous-finalité 2						
Sous-finalité 3						
Sous-finalité 4						
Sous-finalité 5						
Mesures de sécurité						
Mesures de						

89

89

L'analyse d'impact

- Le but
- Notion de risque et évaluation du risque
- Les mesures de gestion du risque
- L'outil de la CNIL

90

90

L'article 35 du RGPD prévoit la conduite d'une analyse d'impact relative à la protection des données (AIPD - Data Protection Impact Assessment), **lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés** des personnes concernées.

91

91

Le but

Une fois la description du traitement réalisée, l'AIPD repose sur deux piliers :

- l'évaluation, (nature axée « **juridique** ») de la nécessité et de la proportionnalité concernant les principes et droits fondamentaux (finalité, données et durées de conservation, information et droits des personnes, etc.) non négociables, qui sont fixés par la loi et doivent être respectés, quelle que soit la nature, gravité et vraisemblance des risques ;

- l'étude, (nature **plus technique**), des risques sur la sécurité des données (accès non autorisé, modification et disparition de données, et leurs impacts potentiels sur la vie privée), qui permet de déterminer les mesures techniques et d'organisation pour protéger les données.

92

92

La notion de « risque »

Un « risque sur la vie privée » est un scénario décrivant :

- un événement redouté (accès non autorisé, modification non désirée ou disparition de données, et ses impacts potentiels sur les droits et libertés des personnes) ;

- toutes les menaces qui permettraient qu'il survienne.

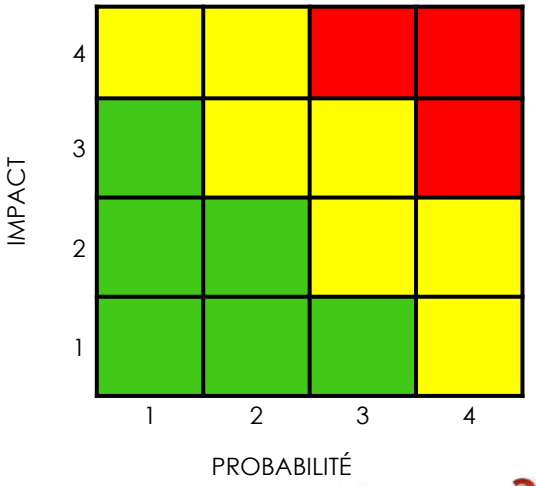
IMPACT X PROBABILITÉ= IMPORTANCE DU RISQUE

93

93

L'évaluation du risque

IMPACT	
1	Impact négligeable: les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, sans difficulte
2	Impact limité: les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourraient surmonter malgré quelques difficultés
3	Impact important: les personnes concernées pourraient connaître des conséquences significatives, qu'elles pourraient surmonter, mais avec de sérieuses difficultés
4	Impact maximal: les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter

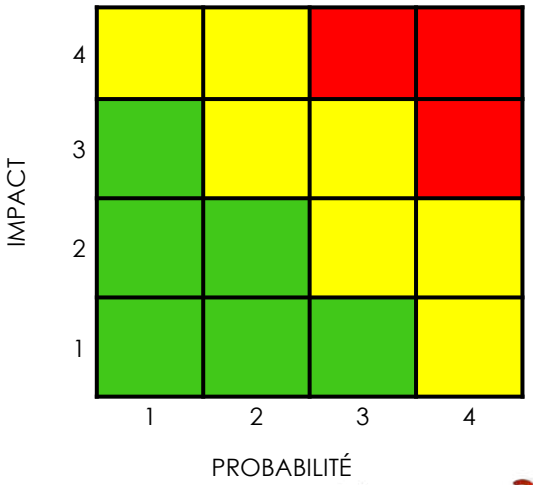


94

94

L'évaluation du risque

PROBABILITÉ	
1	La probabilité que le risque se déclenche est négligeable (jamais dans les deux dernières années)
2	La probabilité que le risque se déclenche est mesuré (une fois dans les deux dernières années)
3	La probabilité que le risque se déclenche est significatif (une fois dans la dernière année)
4	La probabilité que le risque se déclenche est important (plusieurs fois dans la dernière année)



95

95

Analyse d'impact. Obligatoire?

Une AIPD doit obligatoirement être mené quand le traitement est «susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées ».

Analyse d'impact si au moins 2 des critères suivants réunis:

- évaluation/scoring (y compris le profilage) ;
- décision automatique avec effet légal ou similaire ;
- surveillance systématique ;
- collecte de données sensibles ;
- collecte de données personnelles à large échelle ;
- croisement de données ;
- personnes vulnérables (patients, personnes âgées, enfants, etc.) ;
- usage innovant (utilisation d'une nouvelle technologie) ;
- exclusion du bénéfice d'un droit/contrat.

96

96

Qui réalise l'analyse d'impact?

Les acteurs clés

Le responsable de traitement = s'assure de la conformité de son traitement au RGPD.

S'il a désigné **un délégué à la protection des données** = conseil et vérification de l'exécution de l'AIPD.

Si un **sous-traitant** intervient dans le traitement = il fournit son aide et les informations nécessaires à la réalisation de l'AIPD.

97

97

Qui réalise l'analyse d'impact?

Les acteurs supports

Demander l'avis des **personnes concernées** (par le biais d'une enquête, d'un sondage, d'une question formelle aux représentants du personnel), ou le justifier sinon.

Les métiers (maîtrise d'ouvrage), **les équipes** chargées de la mise en œuvre (maîtrise d'œuvre), et la personne chargée de la **sécurité des systèmes d'information** devraient également participer au processus de réalisation de l'AIPD et à sa validation.

98

98

Outils pour le PIA

OUTIL DE LA CNIL

103

103

PIA de la CNIL

Le Privacy Impact Assessment

Téléchargement libre

104

104

Les mesures pour optimiser la sécurisation des données

- Les sauvegardes
- Le chiffrement
- Anonymisation / Pseudonymisation
- La responsabilisation
- Le contrôle
- La sensibilisation

105

105

Les sauvegardes

- Internes et/ou externes (serveur ou disque externe)
- Programmées (service informatique), sur un serveur (local ou cloud) et/ou manuelles (clés/disques)
- Régulières (automatiquement via le SI ou hebdomadaires sur disques)
- Les informations concernant les sauvegardes sont à renseigner dans les registres

INDISPENSABLE

106

106

Le chiffrement

- Utilisation d'applications payantes ou gratuites
- Principe: rendre un dossier ou un fichier **illisible** en appliquant un algorithme défini par un mot de passe
- Options: rendre le dossier ou fichier **invisible** **(**exemple avec VeraCrypt**)**

>conseillé par la **CNIL**

AxCrypt
www.axcrypt.net

VeraCrypt
https://www.veracrypt.fr/en/Downloads.html

IMPORTANT

107

107

Anonymisation / Pseudonymisation

L'anonymisation = empêcher l'identification d'une donnée de manière **irréversible**.

Hors champ d'application RGPD

La pseudonymisation = technique de sécurisation **réversible**, (réduction du lien de corrélation entre les données d'identification et les autres données d'une personne).

108

108

La responsabilisation

Clauses de confidentialité

Engagement des différentes parties à respecter les données (notamment personnelles) dans le cadre de la relation professionnelle, donc pas de divulgation, pas de revente, pas de duplication

Attestation de reconnaissance de responsabilité

Reconnaissance des parties utilisant les données du caractère responsabilisant de leur mission. Donc faire prendre conscience que toute divulgation, modification, destruction volontaire, accidentelle ou non peut amener à des poursuites dans le respect de la loi.

Articles 226-16 à 226-24 du code pénal

109

109

Le contrôle

INTERNES

- **Audits internes programmés (par le DPD – délégué à la protection des données)**
- **Contrôles internes par les responsables de traitement**
- **Autocontrôles**

EXTERNE

- **Par la CNIL:**
  - **Démontrer l'existence, la tenue et la mise à jour du registre de traitement**
  - **Démontrer l'existence et l'utilisation des procédures préventives de manipulation des données**
  - **PIA si nécessaire**

110

110

Les sanctions

Avec le **RGPD** (Règlement Général sur la Protection des Données), le montant des **sanctions** pécuniaires peut s'élever jusqu'à 20 millions d'euros ou dans le cas d'une entreprise jusqu'à 4 % du chiffre d'affaires annuel mondial. Ces **sanctions** peuvent être rendues publiques.

111

111

Les Grandes entreprises dans le viseur

Carrefour : 3 millions € pour ne pas avoir informé les personnes de leurs droits

H&M : 35 millions d'euros pour surveillance illégale de ses employés

Marriott : 20 millions pour ne pas avoir sécurisé ses données

Google / Amazon : 135 millions d'euros pour violation des règles en matière de cookies

112

112

Spartoo (vente en ligne de chaussures) : 250.000€ pour collecte illégale de données

LES PME ET TPE également concernées

Une App mobile sanctionnée à 20.000€ pour envoi d'email intempestifs

112.000€ de sanctions pour un hôpital n'ayant pas protégé les données de patients

7.500€ de sanctions pour une TPE (Perfoclick) ayant spammé ses utilisateurs

Deux médecins sanctionnés à 9.000€ pour ne pas avoir protégé des données médicales

113

113

La sensibilisation

- **Caractère OBLIGATOIRE, périodique et régulier**
- **L'ensemble des collaborateurs concernés**
- **Le rappel des règles de protection des données**
- **Les risques actuels (cybercriminalité, risques humains, terrain, informatiques)**
- **L'affaire de tous… le DPD est le chef d'orchestre et centralise les opérations**

114

114

8 Règles d'OR RGPD

- ✓Licéité du traitement
- ✓Finalité du traitement
- ✓Minimisation des données
- ✓Protection des données sensibles
- ✓Conservation limitée des données
- ✓Obligation de sécurité et confidentialité
- ✓Transparence
- ✓Respect des droits des personnes

115

115

Résumé des actions

1. Désignation d'un **DPD**
2. Mise en place d'un **registre de traitement des activités**
3. Si données sensibles : **analyse d'impact**
4. Mise en place des **restrictions d'accès**
5. **Sensibilisation**

116

116

IFCE
MS2 Mngt projet Marketing

Sensibilisation
Protection du patrimoine
Sécurisation des données

117

117

PLAN

- Catégorisation des menaces
- Type de risques et comment les contrôler
- Sensibilisation

118

118

Sécurité des systèmes d'information:

- **Intégrité**
- **Disponibilité**
- **Confidentialité**

Enjeu: protéger les données de l'entreprise.

« **63% de la valeur des entreprises étudiées correspond à de l'immatériel** »

Source : ERNST & YOUNG.

119

119

Sécurité de l'information

« ***l'ensemble des actions et des procédures conçues pour prévenir, avec un niveau de certitude démontrable, la divulgation, le transfert, la modification ou la destruction non autorisée, volontaire ou accidentelle de données.*** »

Source : SSI-CONSEIL

Avoir à l'esprit le « besoin d'en connaître… »

120

120

Types de risques et comment les contrôler

Les risques, qui peuvent être externes ou internes sont de plusieurs types:

- Le risque humain
- Le risque terrain
- Le risque informatique

122

122

Le risque humain:

- La méconnaissance environnementale
- L'imprudence
- La duperie
- Ingénierie sociale
- BYOD

123

123

Comment prévenir le risque humain:

- La sensibilisation
- La formation
- La responsabilisation
- La protection des personnes
- Distinguer le « Nice to Know » et le « Need to Know »

124

124

Le risque terrain:

- Les accès non sécurisés
- Les vols (échantillons,…)
- Le sabotage d'outils de production
- Les SPC (Signaux Parasites Compromettants)

125

125

Comment prévenir le risque terrain:

- La mise en place d'accès sécurisés
- L'accompagnement des visiteurs et stagiaires
- La prise en compte environnementale
- Le respect des règles de conservation de données sensibles

126

126

Et les déplacements???

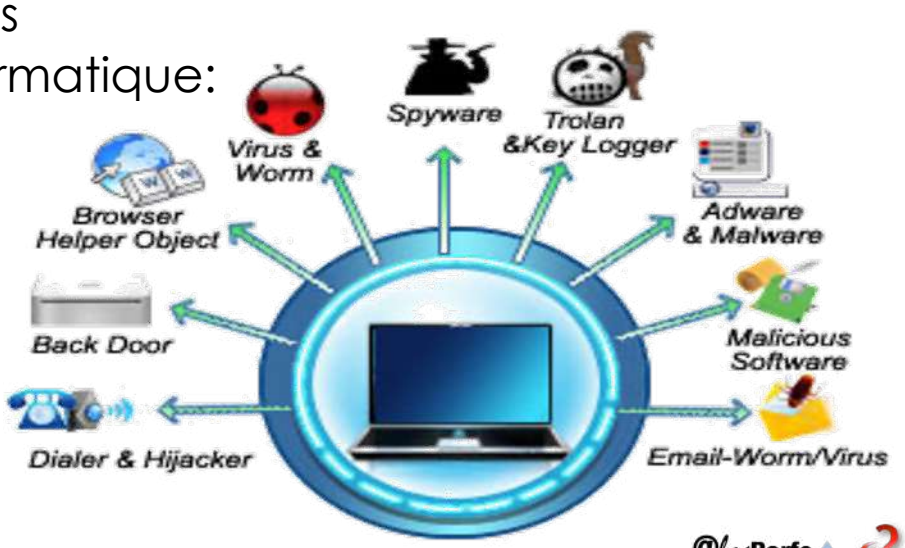
- Cybercafés, les hôtels, les lieux publics n'offrent pas de garantie de confidentialité.
- Utiliser du matériel dédié aux déplacements ne comprenant que le stricte nécessaire à la mission

127

127

Types de risques

Le risque informatique:

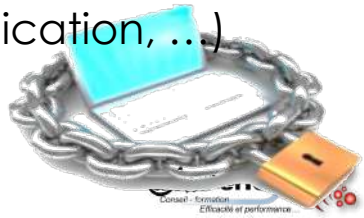


128

128

Comment prévenir et limiter le risque informatique:

- La mise en place d'une politique de sécurisation des informations numériques
- La sensibilisation, la communication
- La présence d'un responsable de la sécurité des systèmes d'information
- Le respect des règles de manipulation de données numériques (transmission, chiffrage, duplication, …)



129

129

- Mots de passe

Identification
= le login

+

Authentification
= le mot de passe

=

130

130

- **1** mot de passe unique pour **chaque service**.
- Choisissez un mot de passe qui **n'a pas de lien avec vous.**
- **Ne demandez jamais à un tiers** de générer pour vous un mot de passe.
- Modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent.
- Renouvelez vos mots de passe avec une fréquence raisonnable.
- Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle.
- Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se « souviennent » pas des mots de passe choisis.
- 12 caractères avec Maj, Min, chiffres, caractères spéciaux.

131

131

https://password.kaspersky.com/fr/

https://haveibeenpwned.com/

- La méthode phonétique :

« J'ai acheté 2 kg de pdt pour 4 euros cet après-midi » = ght2KgPdT4€7am ;

- La méthode des premières lettres

« un tien vaut mieux que deux tu l'auras » = 1tvmQ2tl'A.

132

132

- Faux profils et réseaux sociaux
- Objectif : intrusion

133

133

Créer un faux profil: à la portée de tout le monde

134

134

Donc attention!! Tout le monde n'est pas ami…

135

135

Donc attention!! Après 2 jours…

136

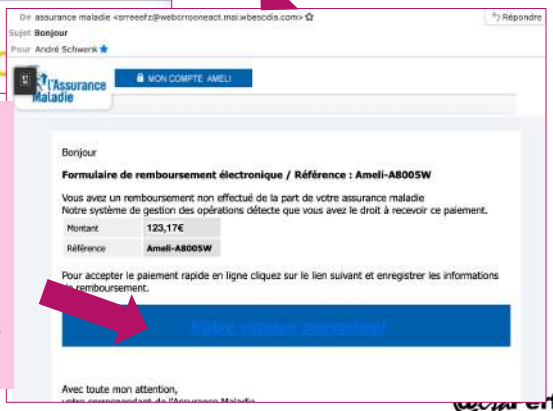
136

- Phishing
- Objectif : récupérer les identifiants

137

137

Adresse mail incohérente?
Proposition de remboursement?
Demande d'identifiants?



Ne pas ouvrir les pièces jointes
Supprimer le message
Vider la corbeille

<u>Plus globalement</u>:
Attention à l'endroit où l'on s'inscrit
Ne rien donner via message
Minimiser les informations fournies sur les formulaires

138

138

▶Clé USB

139

139

Les dangers :

Présence d'un « autorun »
Présence d'un Key logger
Présence de tout logiciel malveillant

Comment s'en prémunir

Gestion des droits d'accès au port USB
Ne pas être impatient de voir ce qui se trouve sur la clé…
Se méfier d'une clé trouvée « par hasard »
Utiliser l'antivirus

140

140

141

- Ransomware – enjeux pour l'entreprise
- Objectif : FINANCIER

142

142

Principe de fonctionnement:
Petit programme malveillant téléchargé sur son poste, qui, lorsqu'il se déclenche, chiffre les données.
Ces dernières sont inutilisables si on ne paye pas la rançon demandée.

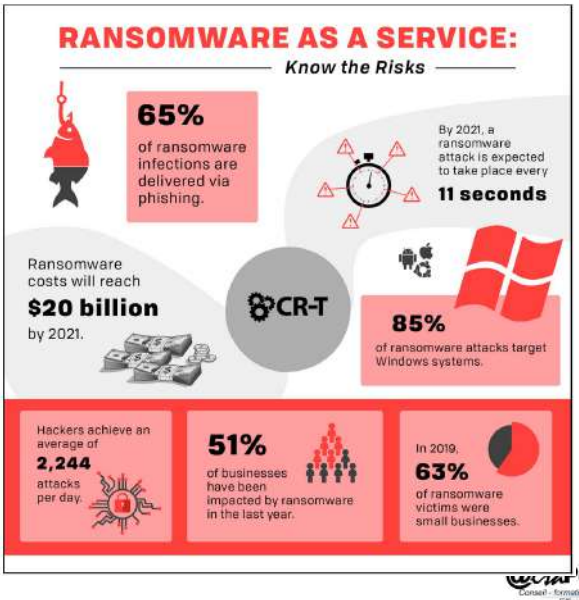
Infection par:
Clic sur une PJ
Clic sur un lien
Transmission par clé USB
Via la stéganographie (fichier caché dans un autre fichier apparemment sain)

- Se débrancher du réseau, appeler le RSSI
- Ne pas payer la rançon demandée
- Sauvegarder, sauvegarder et sauvegarder encore
- Mise à jour de son antivirus et de ses applications

143

Sur le « dark web… » un supermarché pour les cybercriminels

La question n'est plus est ce que cela va m'arriver, la question est QUAND?



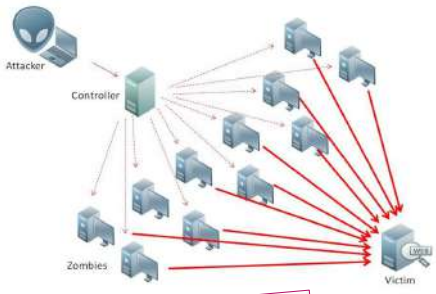
144

- Botnet
- DDoS (Distributed Denial of Service)
- Objectif : BLOCAGE

145

une attaque DoS va chercher à rendre indisponible un site ou un service Web (surcharger la cible d'un nombre de requêtes si important qu'elle sera rendue indisponible).

Les motivations: politiques, militantes (on parle d'hacktivisme), financières ou tout simplement dans une quête d'exploit médiatique.



Accueil > News > OVH

OVH noyé par une attaque Ddos sans précédent

Sécurité : *L'hébergeur roubaisien a fait face à une attaque Ddos d'ampleur ayant dépassé la barre du térabit par seconde. À l'origine de cette offensive, un botnet de caméras IP infectées par des cybercriminels.*

Par La rédaction de ZDNet.fr | Modifié le mardi 27 sept. 2016 à 17:00

146

Conseils:

Respecter les consignes du RSSI
Sauvegarder

Réfléchir avant d'ouvrir une pièce jointe

Adopter les réflexes de contrôle et d'utilisation des antivirus
Sauvegarder

En cas de doute: demander

Sécuriser sa vie, pour ne pas mettre en péril bien plus que sa propre vie…

Je ne sais pas si je l'ai déjà dit : **sauvegarder !!**

Avoir du bon sens

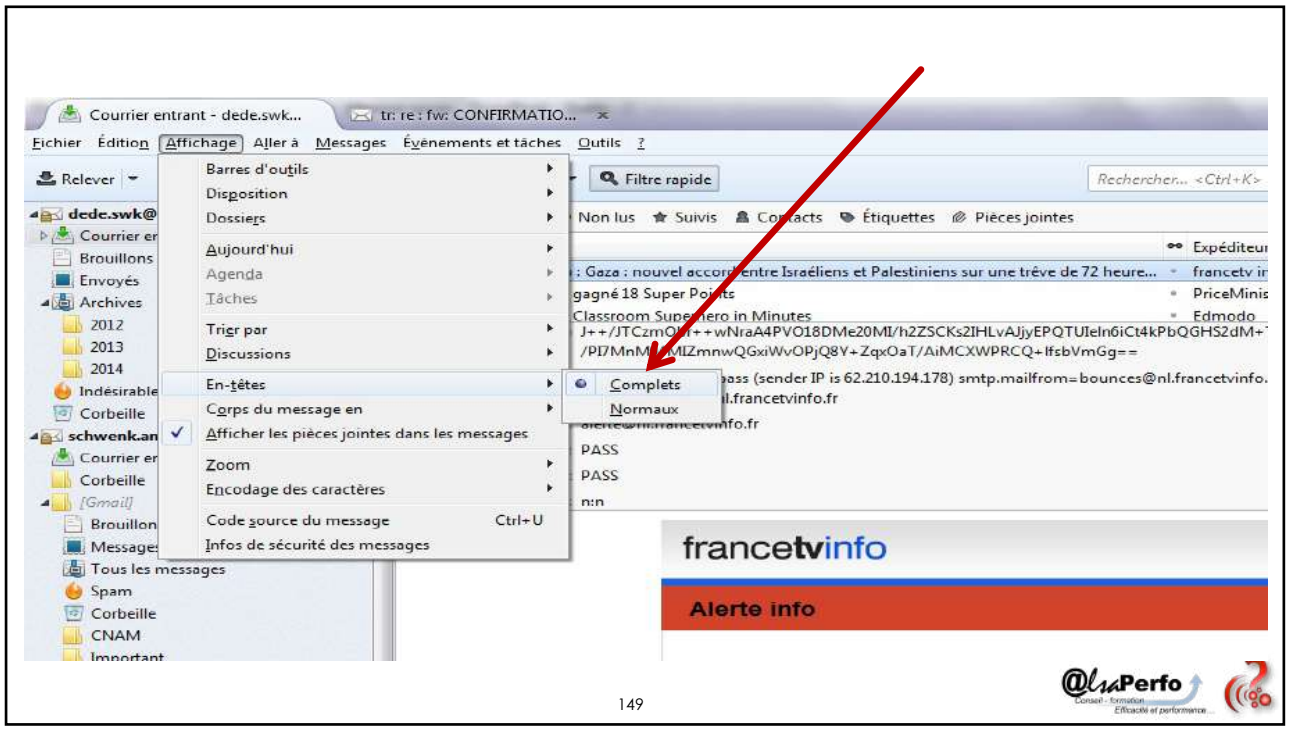
147

Quelques outils

Antivirus
FireWall
Ccleaner
AxCrypt
TrueCrypt
VeraCrypt
Malwarebytes
AdwCleaner

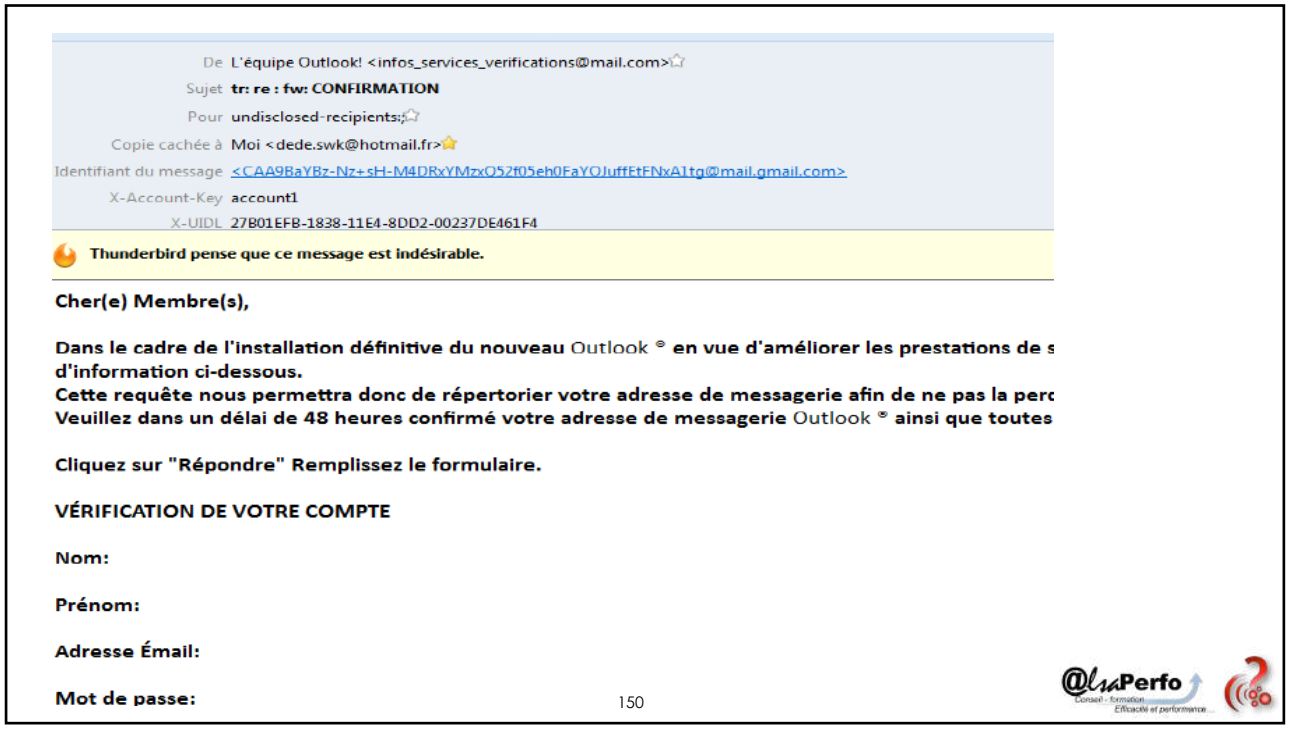
148

148



149

149



150

150

Si on parlait réseaux sociaux…

151

151

Conseils pour les réseaux sociaux…

Disposer d'un compte, même inactif (pour éviter l'usurpation d'identité)

Sélectionner rigoureusement les contacts….tout le monde n'est pas « ami »!!:

Vos mots de passe : choisir des mots de passe différents de ceux de votre messagerie

Attention: les informations en ligne sont publiques et à vie

Respecter le devoir de réserve

Cas des photos (notamment celles des enfants)

Dissocier compte privé et compte professionnelle

152

152

L'arnaque au Président

Michelin victime de « l'arnaque au président »

LES ECHOS | LE 03/11 À 21:20, MIS À JOUR LE 04/11 À 10:41

Michelin s'est fait dérober quelque 1,6 million d'euros - AFP

1 / 1

153

153

Darkhotel

Les dirigeants d'entreprises espionnés grâce au Wi-Fi des hôtels

> ECONOMIE > HIGH-TECH Par Fawaz Teffahi | Mis à jour le 12/11/2014 à 17:48 | Publié le 12/11/2014 à 17:27

154

154

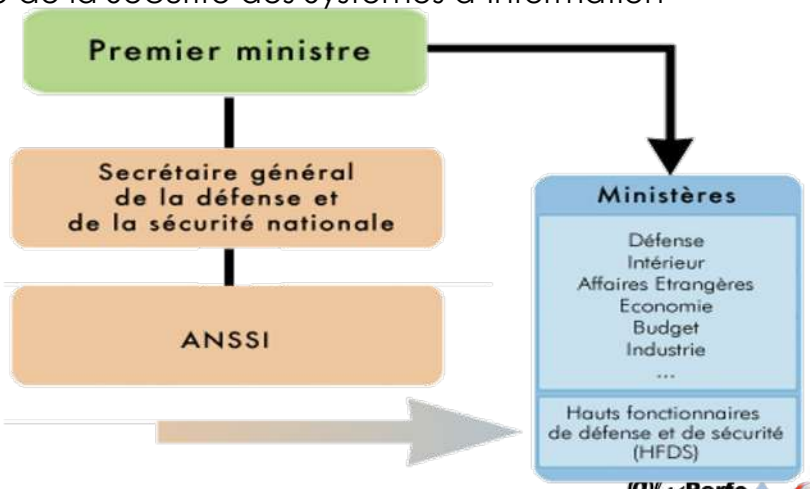
Kaspersky cyberthreat map

155

156

Organisation

ANSSI: Agence Nationale de la Sécurité des Systèmes d'Information
http://www.ssi.gouv.fr/



157

157

Lien utile…

http://cert.ssi.gouv.fr/

158

158

Tout doit se protéger, et ce n'est souvent que du bon sens…
L'information la plus anodine peut contribuer à terminer le puzzle…

159

159

« lorsque vous fermez la porte d'un laboratoire, vous enfermez plus de choses à l'extérieur qu'à l'intérieur »

Louis Pasteur

160

160

Les grands principes du RGPD

La licéité et la loyauté
Les données doivent être traitées de façon licite, loyale, et transparente.

La limitation des finalités
Les données sont collectées pour des finalités déterminées, explicites et légitimes.

La pertinence des données
Seules les données nécessaires à la réalisation de la finalité peuvent être traitées.

L'exactitude des données
Les données doivent être exactes, et régulièrement mises à jour.

La conservation limitée des données
Une fois la finalité atteinte, les données ne doivent pas être conservées.

La sécurité des données
Les données doivent être protégées contre le traitement illicite, la perte et la destruction

161

161

FIN de la présentation, maintenant, à vous de jouer

162

162