CLUB DECOM VALAIS

AVANSIS
SOLUTIONS D'INTEGRATION
& CYBER-SECURITE

Cyber-risques:
Etat des lieux et protection des données

Avansis Sàrl – Rte de Sion 1 / CP 8 – 3960 Sierre
T. +41(0)27 455 37 62 – w. www.avansis.ch – m. info@avansis.ch

Contact

Marie Zuchuat

Responsable Compliance & Anti-blanchiment

Conseillère à la protection des données de la BCVs

marie.zuchuat@bcvs.ch

Tel: 058/324.66.06

08.03.2019

Jérôme Christen

AVANSIS
SOLUTIONS D'INTEGRATION
& CYBER-SECURITE

Fondateur et directeur d'Avansis sàrl

Consultant en sécurité informatique
Formateur à la HESSO
Chef de projet marketing digital

jchristen@avansis.ch
Tel: 079 4362159

Vols de mots de passe: Collection #1-5

RTS INFO

https://www.rts.ch/info/suisse/10266741-de-larmee-au-conseil-federal-toute-la-suisse-concernee-par-une-fuite-de-donnees.html

Le Cyber-crime

- Marché du Cyber-crime:
  500 milliards $ en 2017
  (source Microsoft)
  400 milliards $ en 2014
  (source Allianz)

- Cryptowall a gagné **325 millions $ aux USA en 2015**

- Le Cyber-crime coûte **600 milliards $** par année à l'économie mondiale

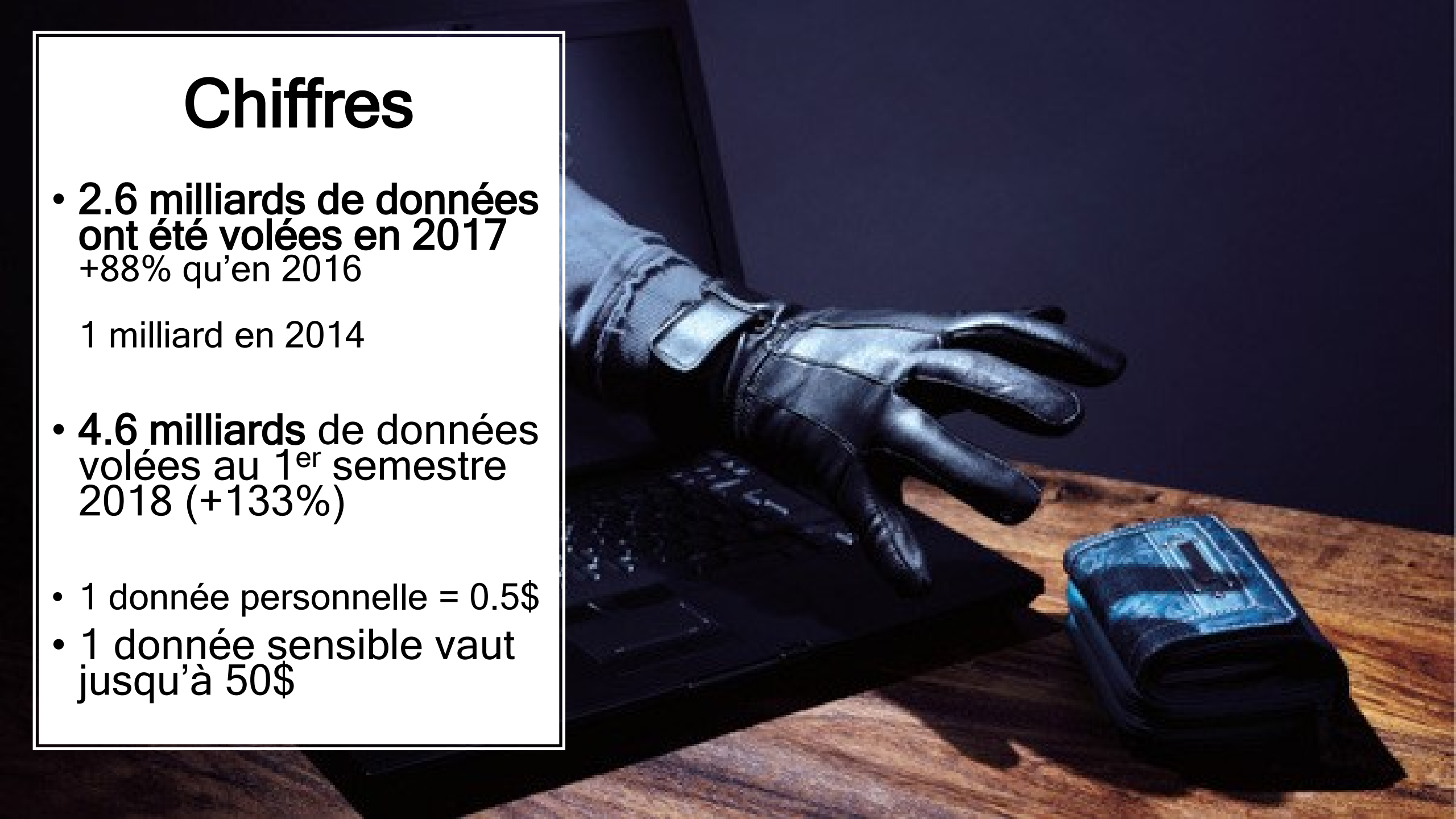
Chiffres

- **2.6 milliards de données ont été volées en 2017**
  +88% qu'en 2016

  1 milliard en 2014

- **4.6 milliards** de données volées au 1er semestre 2018 (+133%)

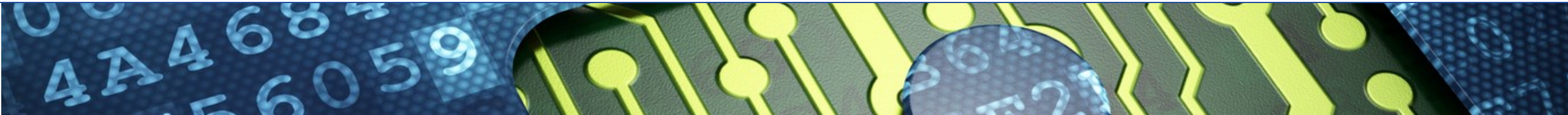
- 1 donnée personnelle = 0.5$
- 1 donnée sensible vaut jusqu'à 50$



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Loi fédérale sur la
Protection des
Données

Révision en 2019

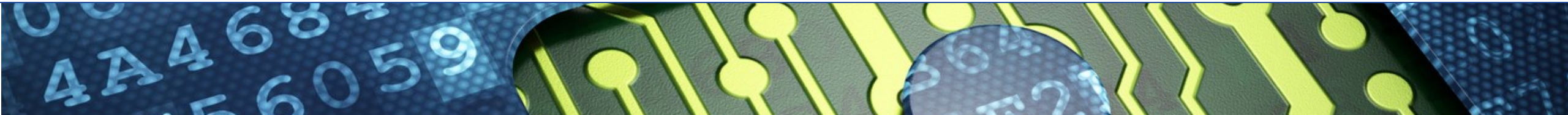


Conséquences concrètes

Unfortunately, our website is currently unavailable in most European countries. We are engaged on the issue and committed to looking at options that support our full range of digital offerings to the EU market. We continue to identify technical compliance solutions that will provide all readers with our award-winning journalism.

LA TIMES

What the LA Times says when you click on its site from certain European countries



Sanctions - 1 an après

- 59’000 plaintes
- 91 amendes (aucune en Suisse à ce jour)

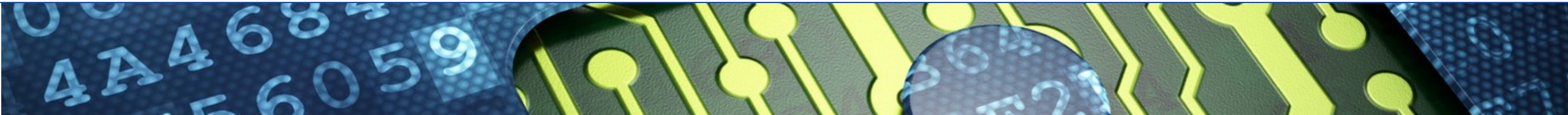
Pays	Société	Motif	Amende
France	Optical Center	Sécurité des données des clients du site web	250’000 €
France	Daily Motion	Atteinte à la sécurité des données	50’000 €
USA	Uber	Atteinte à la sécurité des données	400’000 €
USA	Google	Manque de transparence, absence de consentement pour la personnalisation de la publicité	50’000’000 € (0.051% CA)

Qui est-ce que cela concerne?

- Les entreprise suisses traitant des données de citoyens de l'UE
- Les entreprises suisses ayant une succursale dans l'UE

- Les clients
- Les employés
- Les fournisseurs / sous-traitants

- Votre vie privée personnelle



Sécurité

Proportionnalité Finalité

Reconnaissabilité

Consentement

Communication

Privacy by Default

Légalité

Bonne foi

Privacy by Design

Droit à l'oubli

Exactitude

Droit à l'accès

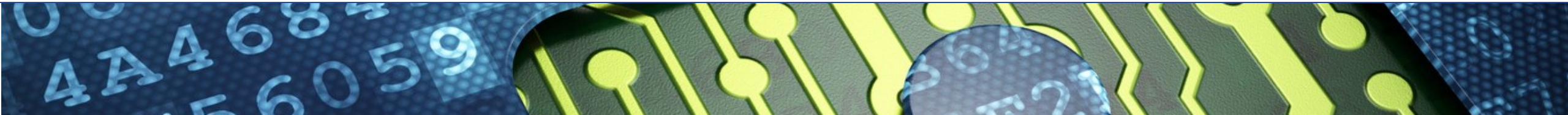
Information Centric Security

Privacy by Design (protection des données dès la conception)

Impose au responsable du traitement de concevoir dès l'origine le traitement des données de telle manière qu'il respecte les prescriptions relatives à la protection des données, en prenant toute mesures technique propre à permettre la protection des données personnelles

Privacy by Default (protection des données par défaut)

Impose au responsable du traitement de garantir que le traitement des données est limité au minimum requis par le but poursuivi et de laisser à la personne concernée la possibilité de modifier les paramètres



Information Centric Security

Registre des activités de traitement

Toutes les activités de traitement de données doivent être enregistrées. Ce registre devra être mis à disposition de l'autorité. S'il y a moins de 250 employés une version simplifiée suffit

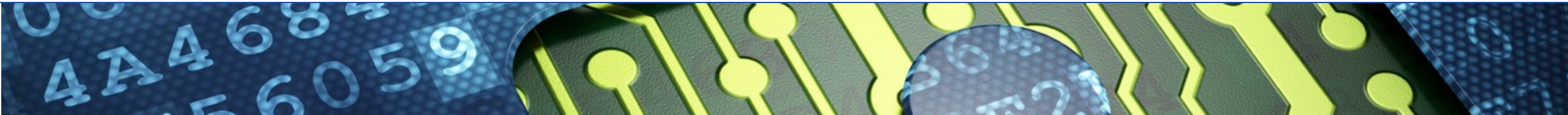
Analyse d'impact relatif à la PD

(Private Impact Assessment)

Lorsqu'un traitement induit un risque élevé pour les personnes concernées

Obligation de notifier lors de violation

Notifier l'organe de contrôle concerné et dans certains cas les personnes concernées

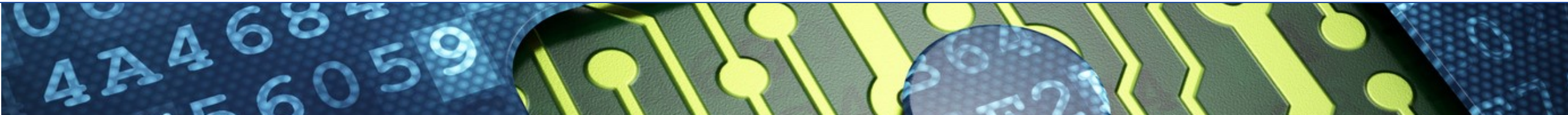


Communication en cas de vol de données

- Notification à l'organe de surveillance
  - 72 heures pour la RGPD, au mieux pour la LPD

- Communication aux personnes concernées
  (s'il y a un risque important pour ses droits)

- Corrections des problèmes techniques
  - Gérer et corriger le problème en cours
  - Empêcher que le problème ne se reproduise
  - Améliorer la détection des attaques

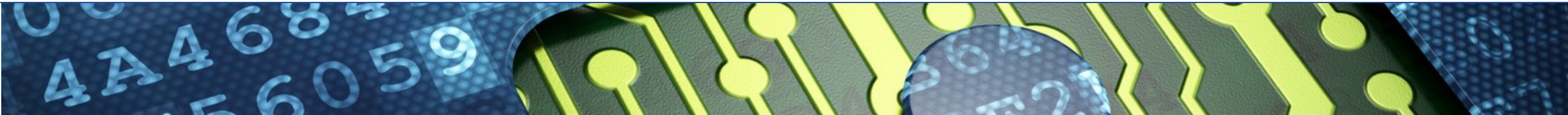


Les rôles de la protection des données
DPO

(Data Protection Officer / Délégué à la Protection des Données)

- " chef d'orchestre" de la conformité

- Informer et conseiller l'entreprise
- Contrôler le respect des normes de la protection des données
- Coopérer avec les autorités compétentes
- Répondre aux personnes concernées
- Gérer le fichier central des registres



Cyber risques, les enjeux de la communication

CLUB DECOM VALAIS

PRÉSENTATION DU 07 MARS 2019

Marie Zuchuat
Responsable compliance &
Conseillère à la protection des données

BCVS | WKB

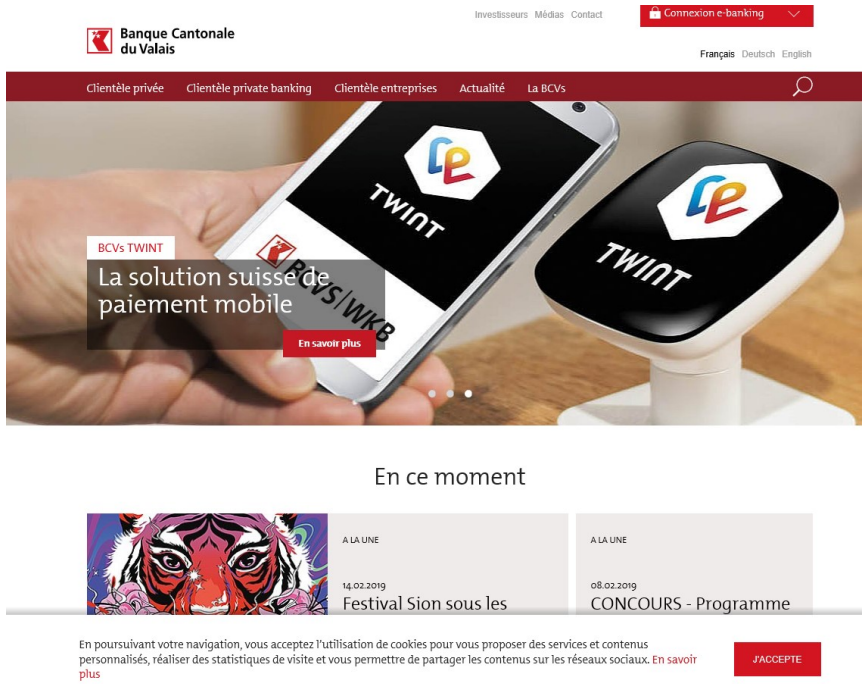
RGPD Impact sur la communication

- Domaine qui recueille beaucoup de données personnelles (mailing, formulaire,…)

- Principe en un mot-clé : **Le Consentement de la personne**

- Bonnes pratiques à suivre :
  - pas de case cochée par défaut
  - texte clair et précis
  - formulaires indépendants
  - système double opt-in
  - information sur profilage / possibilité de refuser
  - politique de protection des données facilement accessible
  - consentements vérifiés et mis à jour
  - prestataires en conformité

Mise en pratique - exemples



Une première mesure:

- Mise en place d'une déclaration de consentement
- Utilisation des cookies

En poursuivant votre navigation, vous acceptez l'utilisation de cookies pour vous proposer des services et contenus personnalisés, réaliser des statistiques de visite et vous permettre de partager les contenus sur les réseaux sociaux. En savoir plus

J'ACCEPTE

08.03.2019

Mise en pratique - Politique de confidentialité

BCVS | WKB

Politique de confidentialité

Préambule

Le document « Informations juridiques » stipule qu'en consultant le site internet de la Banque Cantonale du Valais (ci-après : le « Site »), vous donnez votre consentement à la Banque Cantonale du Valais (ci-après : la « BCVs ») pour la collecte, le traitement et la transmission éventuelle de vos données selon les termes de la Politique de confidentialité. La présente Politique de confidentialité de la BCVs complète ainsi les « Informations juridiques » et s'applique dès que vous vous connectez au Site, quel que soit le type d'accès, lorsque vous utilisez le Site et les pages qu'il contient.

Données personnelles collectées

Toutes les données personnelles transmises par l'utilisateur du Site (ci-après : les « Données ») sont traitées conformément aux dispositions de la Loi fédérale sur la protection des données (LPD).

La BCVs peut collecter des Données par le biais de son Site si vous mettez expressément vos Données à sa disposition en remplissant un formulaire ou par un autre moyen. Les renseignements requis par la BCVs lors de l'inscription en ligne à un service spécifique offert par celle-ci sont limités aux informations qui lui sont nécessaires pour lui permettre d'assurer le meilleur service et suivi possible.

Finalités du traitement des Données

De manière générale, le traitement des Données par la BCVs est réalisé pour les finalités suivantes (ci-après : les « Finalités ») : la gestion de la relation bancaire et l'exécution de toute opération s'y rapportant, la gestion des comptes ou des produits ou des services souscrits, la gestion des risques, la prévention des abus et des fraudes, la sécurisation des canaux de communication, la réalisation de statistiques et de tests, le respect de ses obligations légales et réglementaires (notamment la lutte contre le blanchiment d'argent, la lutte contre le financement du terrorisme, le respect des listes de sanctions financières internationales et embargos), la détermination du statut fiscal, le recouvrement ou cession de créances, et le développement d'offres commerciales et d'opérations marketing. Le but du traitement des Données est de vous fournir les meilleurs services possibles dans le cadre des relations contractuelles (crédit, financement, compte épargne, etc.) ou

Cantonale du Valais (ci-après : le « Site »), vous donnez votre consentement à la Banque Cantonale du Valais (ci-après : la « BCVs ») pour la collecte, le traitement et la transmission éventuelle de vos données selon les termes de la Politique de confidentialité. La présente Politique de confidentialité

LPD

Toutes les données personnelles transmises par l'utilisateur du Site (ci-après : les « Données ») sont traitées conformément aux dispositions de la Loi fédérale sur la protection des données (LPD).

Limite

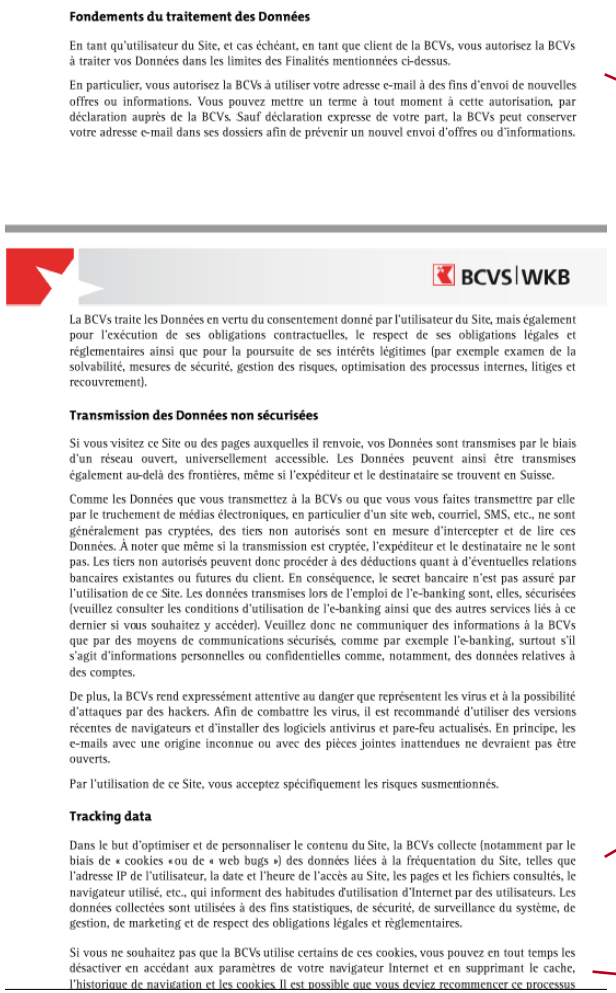
requis par la BCVs lors de l'inscription en ligne à un service spécifique offert par celle-ci sont limités aux informations qui lui sont nécessaires pour lui permettre d'assurer le meilleur service et suivi possible.

But

marketing. Le but du traitement des Données est de vous fournir les meilleurs services possibles dans le cadre des relations contractuelles (crédit, financement, compte épargne, etc.) ou extracontractuelles (marketing, statistiques, sécurité, etc.) que la BCVs entretient avec vous, mais également de se conformer à toutes les règles en vigueur qui affectent le domaine bancaire.

08.03.2019

Mise en pratique - exemples



Fondements du traitement des Données

En tant qu'utilisateur du Site, et cas échéant, en tant que client de la BCVs, vous autorisez la BCVs à traiter vos Données dans les limites des Finalités mentionnées ci-dessus.

En particulier, vous autorisez la BCVs à utiliser votre adresse e-mail à des fins d'envoi de nouvelles offres ou informations. Vous pouvez mettre un terme à tout moment à cette autorisation, par déclaration auprès de la BCVs. Sauf déclaration expresse de votre part, la BCVs peut conserver votre adresse e-mail dans ses dossiers afin de prévenir un nouvel envoi d'offres ou d'informations.

BCVS | WKB

La BCVs traite les Données en vertu du consentement donné par l'utilisateur du Site, mais également pour l'exécution de ses obligations contractuelles, le respect de ses obligations légales et réglementaires ainsi que pour la poursuite de ses intérêts légitimes (par exemple examen de la solvabilité, mesures de sécurité, gestion des risques, optimisation des processus internes, litiges et recouvrement).

Transmission des Données non sécurisées

Si vous visitez ce Site ou des pages auxquelles il renvoie, vos Données sont transmises par le biais d'un réseau ouvert, universellement accessible. Les Données peuvent ainsi être transmises également au-delà des frontières, même si l'expéditeur et le destinataire se trouvent en Suisse.

Comme les Données que vous transmettez à la BCVs ou que vous vous faites transmettre par elle par le truchement de médias électroniques, en particulier d'un site web, courriel, SMS, etc., ne sont généralement pas cryptées, des tiers non autorisés sont en mesure d'intercepter et de lire ces Données. À noter que même si la transmission est cryptée, l'expéditeur et le destinataire ne le sont pas. Les tiers non autorisés peuvent donc procéder à des déductions quant à d'éventuelles relations bancaires existantes ou futures du client. En conséquence, le secret bancaire n'est pas assuré par l'utilisation de ce Site. Les données transmises lors de l'emploi de l'e-banking sont, elles, sécurisées (veuillez consulter les conditions d'utilisation de l'e-banking ainsi que des autres services liés à ce dernier si vous souhaitez y accéder). Veuillez donc ne communiquer des informations à la BCVs que par des moyens de communications sécurisés, comme par exemple l'e-banking, surtout s'il s'agit d'informations personnelles ou confidentielles comme, notamment, des données relatives à des comptes.

De plus, la BCVs rend expressément attentive au danger que représentent les virus et à la possibilité d'attaques par des hackers. Afin de combattre les virus, il est recommandé d'utiliser des versions récentes de navigateurs et d'installer des logiciels antivirus et pare-feu actualisés. En principe, les e-mails avec une origine inconnue ou avec des pièces jointes inattendues ne devraient pas être ouverts.

Par l'utilisation de ce Site, vous acceptez spécifiquement les risques susmentionnés.

Tracking data

Dans le but d'optimiser et de personnaliser le contenu du Site, la BCVs collecte (notamment par le biais de « cookies «ou de « web bugs ») des données liées à la fréquentation du Site, telles que l'adresse IP de l'utilisateur, la date et l'heure de l'accès au Site, les pages et les fichiers consultés, le navigateur utilisé, etc., qui informent des habitudes d'utilisation d'Internet par des utilisateurs. Les données collectées sont utilisées à des fins statistiques, de sécurité, de surveillance du système, de gestion, de marketing et de respect des obligations légales et règlementaires.

Si vous ne souhaitez pas que la BCVs utilise certains de ces cookies, vous pouvez en tout temps les désactiver en accédant aux paramètres de votre navigateur Internet et en supprimant le cache, l'historique de navigation et les cookies. Il est possible que vous deviez recommencer ce processus

E-mail

En particulier, vous autorisez la BCVs à utiliser votre adresse e-mail à des fins d'envoi de nouvelles offres ou informations. Vous pouvez mettre un terme à tout moment à cette autorisation, par déclaration auprès de la BCVs. Sauf déclaration expresse de votre part, la BCVs peut conserver votre adresse e-mail dans ses dossiers afin de prévenir un nouvel envoi d'offres ou d'informations.

Tracking Data

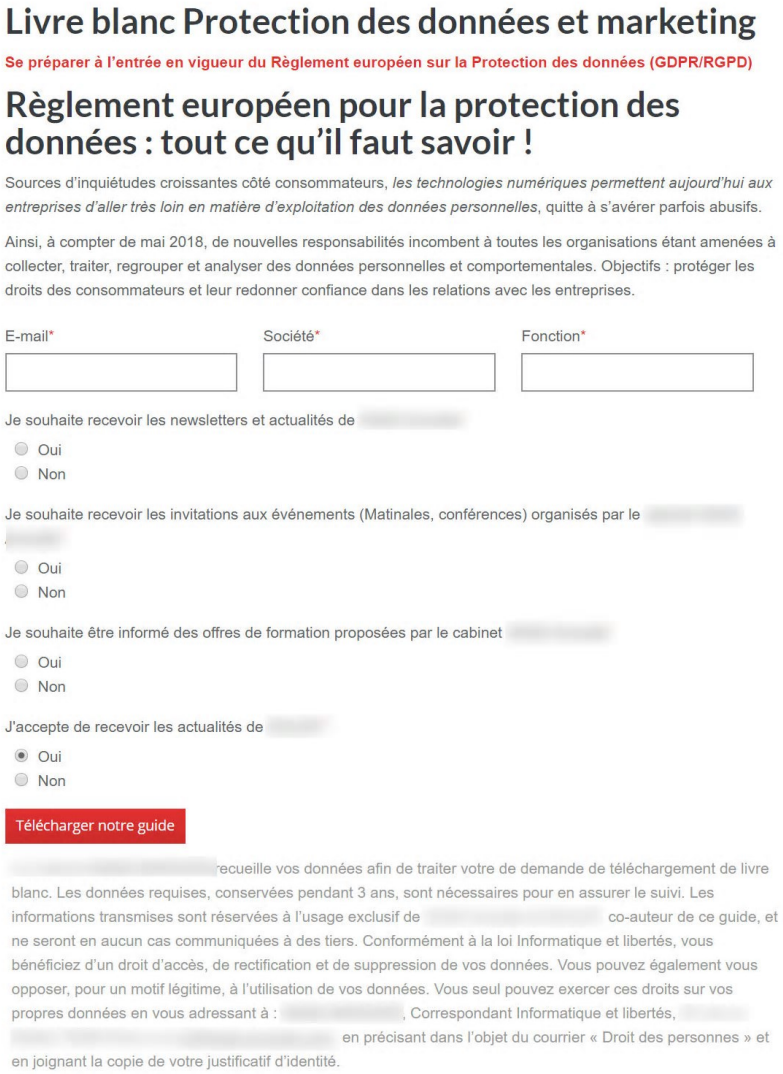
Dans le but d'optimiser et de personnaliser le contenu du Site, la BCVs collecte (notamment par le biais de « cookies « ou de « web bugs ») des données liées à la fréquentation du Site, telles que l'adresse IP de l'utilisateur, la date et l'heure de l'accès au Site, les pages et les fichiers consultés, le navigateur utilisé, etc., qui informent des habitudes d'utilisation d'Internet par des utilisateurs. Les données collectées sont utilisées à des fins statistiques, de sécurité, de surveillance du système, de gestion, de marketing et de respect des obligations légales et règlementaires.

Cookies

Si vous ne souhaitez pas que la BCVs utilise certains de ces cookies, vous pouvez en tout temps les désactiver en accédant aux paramètres de votre navigateur Internet et en supprimant le cache, l'historique de navigation et les cookies. Il est possible que vous deviez recommencer ce processus

08.03.2019

Mise en pratique – exemples formulaires



Mise en pratique – exemples formulaires

Le consentement : opt-in/ opt-out

HAAS AVOCATS

- **Collecte opt-out (case pré-cochée : interdite par RGPD)**

☑ *J'accepte* que mes données soient transférées à des sociétés partenaires.

- **Collecte opt-in (case décochée)**

☐ *J'accepte que mes données soient transférées à des sociétés* partenaires.

L'opt-in est la règle en matière de prospection commerciale (renforcée par le RGPD) !

08.03.2019

Passer à l'action !!!

Vos trois gros chantiers :

1. Réaliser un état des lieux

- Identification et priorisation des départements concernés
- Inventaire et Cartographie des traitements

2. Documenter et mettre en place les procédures internes

- Identification et documentation des bases légales
- Informations et réponses aux personnes concernées et aux autorités publiques
- Clauses contractuelles et accord de niveau de service avec vos partenaires tiers

3. Intégrer les exigences de gouvernance et de politiques internes

- Désignation et justification du DPD (si nécessaire)
- Intégration de la protection dès la conception et analyse des risques
- Revoir les contrôles IT autour des applications pertinentes

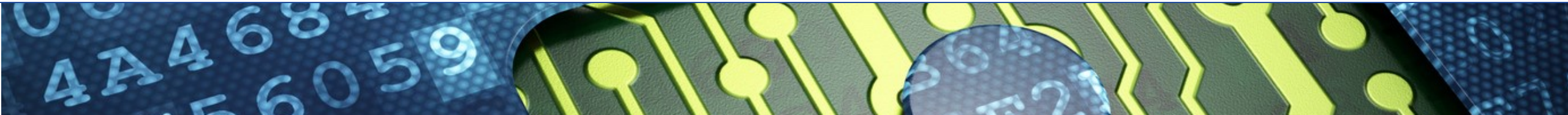
08.03.2019

Formation en entreprise

Formation Continue à la HES-SO Valais-Wallis
http://www.formationcontinue.ch/Nos-cours/Entreprises

Adapter son entreprise au RGPD (02.05.19)
https://www.hevs.ch/fr/hautes-ecoles/haute-ecole-de-gestion-et-tourisme/informatique-de-gestion/autres-formations/formation-continue/cours-entreprise-institution/formations-specifiques/adapter-son-entreprise-au-rgpd-18603

Cyber-sécurité en entreprise (18.03.19)
https://www.hevs.ch/fr/hautes-ecoles/haute-ecole-de-gestion-et-tourisme/informatique-de-gestion/autres-formations/formation-continue/cours-entreprise-institution/internet/securite-informatique-en-entreprise-9093



Conclusion

En informatique, **RIEN** n'est **JAMAIS** sur.

Mettre en place des solutions **AVANT** les problèmes.