La Protection des données

Webinaire du mercredi 28 avril 2021 à 17h00

COMPTAVAL
ASSOCIATION VALAISANNE DES EXPERTS EN FINANCE ET CONTROLLING ET SPECIALISTES EN FINANCE ET COMPTABILITE

Mercredi 28 avril 2021 à 17h00, en direct de Sion

Présentation de ComptaVal

- *Association valaisanne des experts en finance et controlling et des spécialistes en finance et comptabilité*
- *Association fondée en 1972*
- *Plus de 400 membres*
- *Notre rôle :* *- promotion des titres et des intérêts professionnels*
  - Formation et Information
  - Coordination et mise en réseau

Programme 2021

COMPTAVAL
ASSOCIATION VALAISANNE DES EXPERTS EN FINANCE ET CONTROLLING ET SPECIALISTES EN FINANCE ET COMPTABILITE

- *Evénement «Opportunités saisies durant la crise»*
- *Assemblée générale*
- *Réception des lauréats*
- *Séminaire TVA*

Mercredi 28 avril 2021 à 17h00, en direct de Sion

Thème du jour

Règlement général de l'UE sur la protection des données **(RGPD)**

Loi sur la protection des données **(LPD)**

Loi sur les services financiers **(Lsfin)**

Mercredi 28 avril 2021 à 17h00, en direct de Sion

Nos intervenants

Sébastien Fanti

Avocat

Préposé à la protection des données et de la transparence

Yann Corbaz

Avocat

Collaborateur juridique
Ancien General Counsel d'une Banque Privée

Mercredi 28 avril 2021 à 17h00, en direct de Sion

Protection des données, nouveautés consacrées par la LPD

Mardi 28 avril 2021 @Sion

Sommaire de l’exposé

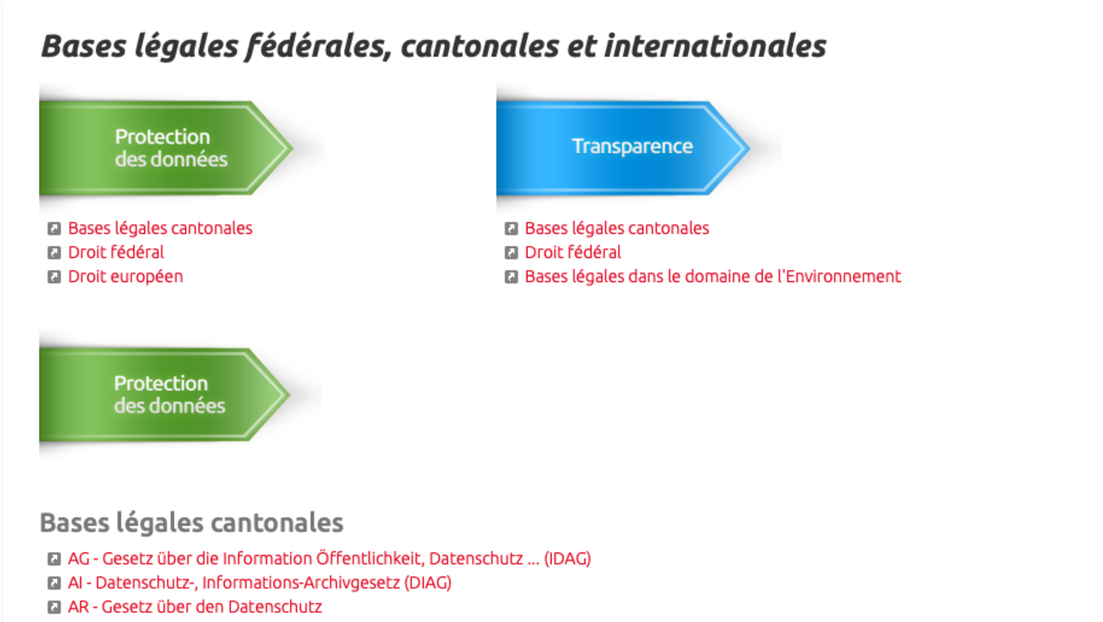
- Contexte
- Principales nouveautés
- Privacy by design et by default
- Conseils et conclusion
- Informations diverses

< Contexte >

- La loi actuelle date de 1992 (entrée en vigueur 1er juillet 1993);
- À cette époque le web venait d'éclore, Google, Facebook, Twitter et consorts n'existaient pas; les collectivités publiques ne disposaient pas encore d'une messagerie électronique…
- Dystocie complexe et longue (trois années de discussion et d'élimination des divergences entre les deux Conseils);
- Résultat dont nous ignorons pour l'heure s'il sera considéré comme conforme aux engagements internationaux de la Suisse! (sanctions, etc.); maintien de l'équivalence à l'aune du RGPD et de la convention 108+?
- Devoirs étendus en matière de transparence et de documentation
- Renforcement de l'Autorité de surveillance et des sanctions

< Contexte >

- Promotion des mesures préventives et responsabilité personnelle des sous-traitants de données
- Développement de dispositions pénales
- La protection des données fait l’objet de normes cantonales et fédérales; il est souvent difficile de déterminer qui est compétent; exemple : LDEP



< Contexte >

- La révision actuelle va engendrer une révision de l'ensemble des normes cantonales en vue de les adapter au droit supérieur : https://drive.google.com/file/d/1f8jHYLU4W8ziA8kiQvxheyDy_SdFbv7a/view

Canton	AG / Aargau	AI / Appenzell Innerrhoden
Dernières informations *(date)*	17/03/2021	((Meldung noch ausstehend))
Concernant la loi		
Nom de la loi *(y c. la date)*	Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen vom 24. Oktober 2006	Datenschutz-, Informations- und Archivgesetz vom 28. April 2019
Forme abrégée, abréviation	IDAG	DIAG
Numéro dans le Recueil systématique	SAR 150.700	GS 172.800
Lien vers la loi dans le Recueil (systématique) des lois	https://gesetzessammlungen.ag.ch/app/de/texts_of_law/150.700	https://ai.clex.ch/frontend/versions/1849?locale=de
Procédure de consultation (publique)		
Etat actuel *(en cours, terminée)*	abgeschlossen	
Lien vers les documents de consultation		
Fin du délai de consultation *(date)*		
Projet/Proposition du Gouvernement au Parlement		
Etat actuel *(pas encore adopté, adopté)*	beschlossen	
Date de l'adoption	23/08/2017	
Nom de la proposition (conseil, message, directive, ...)	Botschaft	
Lien vers la publication de la proposition	s. parlamentarisches Geschäft, 1. Beratung	
Lien vers la publication du projet de loi		
Traitement au Parlement		
Etat actuel *(en délibération, délibération terminée)*	Beratung abgeschlossen	
Lien vers les affaires parlementaires	https://www.ag.ch/grossrat/grweb/de/195/Detail%20Geschäft?ProzId=3566593; https://www.ag.ch/grossrat/grweb/de/195/Detail%20Geschäft?ProzId=3667092	
Rapport de commission: nom		
Rapport de commission: date		
Lien vers un éventuel rapport de commission		

< Nouveautés >

- **Des spécificités suisses existantes ont été conservées.**
- Données personnelles sensibles: élargissement de la notion (données ethniques, génétiques et biométriques)
- Profilage: il s'agit d'un nouveau concept, repris du RGPD; = traitement automatisé de données personnelles relatives par exemple à la santé, à la localisation; il faut le distinguer du profilage à risque élevé qui apparie les données de telle sorte qu'il devient possible d'apprécier les caractéristiques essentielles de la personnalité; un consentement exprès d la personne concernée est nécessaire; analyse des risques de crédit;
- Extension du champ d'application territorial: la loi s'applique aux états de fait qui déploient des effets en Suisse, même s'ils se sont produits à l'étranger;

< Nouveautés >

- Répertoire des activités de traitement des données: obligation du responsable du traitement et du sous-traitant de tenir un répertoire des traitements de données; le CF peut prévoir des exceptions pour les entreprises qui emploient moins de 250 personnes et dont le traitement de données comporte un faible risque de préjudice (cf. OLPD);
- Le transfert d'un traitement de données à un sous-traitant n'est désormais possible qu'avec le consentement préalable du responsable du traitement, de sorte qu'à tout le moins un contrôle indirect est possible; le responsable doit s'assurer que le sous-traitant est en mesure de garantir la sécurité des données; pas d'exigences formelles particulières pour le contrat;

< Nouveautés >

- Droit à la portabilité des données : ce droit permet à la personne concernée d'exiger du responsable du traitement, généralement gratuitement, la communication de ses données personnelles dans un format électronique commun ou leur transfert à un autre responsable du traitement, si le premier responsable traite les données automatiquement et si les données sont traitées avec le consentement de la personne concernée ou en relation directe avec la conclusion ou l'exécution d'un contrat;
- Etude d'impact : le responsable du traitement est tenu de procéder à une évaluation de l'impact sur la protection des données si un traitement de données peut entrainer un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Un risque élevé peut résulter du type, de l'étendue, des circonstances et de la finalité du traitement;

< Nouveautés >

- Notification des violations de la protection des données : nécessité pour le responsable du traitement d'informer le PFPDT dans les plus brefs délais en cas de violation des normes, s'il existe un risque grave pour la personnalité ou pour les droits fondamentaux de la personne concernée; sous certaines exceptions il faut informer la personne concernée; le sous-traitant doit signaler le plus rapidement possible une violation de la sécurité au responsable du traitement (pas au PFPDT ou à la personne concernée)
- Sanctions pénales : les personnes physiques peuvent être condamnées à une amende allant jusqu'à 250'000 francs, notamment en cas de violation intentionnelle des obligions d'information ou de diligence… aucun délai transitoire n'est prévu !

< Privacy by Design >

- Le concept de **Privacy by Design** (développé par Ann Cavoukian) consiste à intégrer des garanties de respect de la vie privée, dans la conception et le fonctionnement des systèmes et réseaux informatiques, tout en y associant des pratiques responsables.
- 7 principes fondamentaux ont été émis:

1)prendre des mesures proactives et non réactives: prévoir et prévenir les incidents

2)assurer la protection implicite de la vie privée: offrir une protection maximale sans nécessité d'intervention

3)intégrer la protection de la vie privée dans la conception des systèmes et des pratiques: la protection des données fait partie du système sans altérer ses fonctions et elle est intégrée à la stratégie et à la pratique

< Fondements >

4) assurer une fonctionnalité intégrale selon un paradigme à somme positive et non nulle: prise en compte de tous les intérêts des partenaires de l'organisation dans une vision positive et constructive
5) assurer la sécurité de bout en bout pendant toute la durée de conservation: conservation et destruction sécurisées
6) assurer la visibilité de la transparence: notamment dans le cadre d'une vérification indépendante
7) respecter la vie privée des utilisateurs: ce qui suppose de concevoir les systèmes informatiques en centrant son approche sur l'utilisateur (Human-Centered Design)

< Fondements >

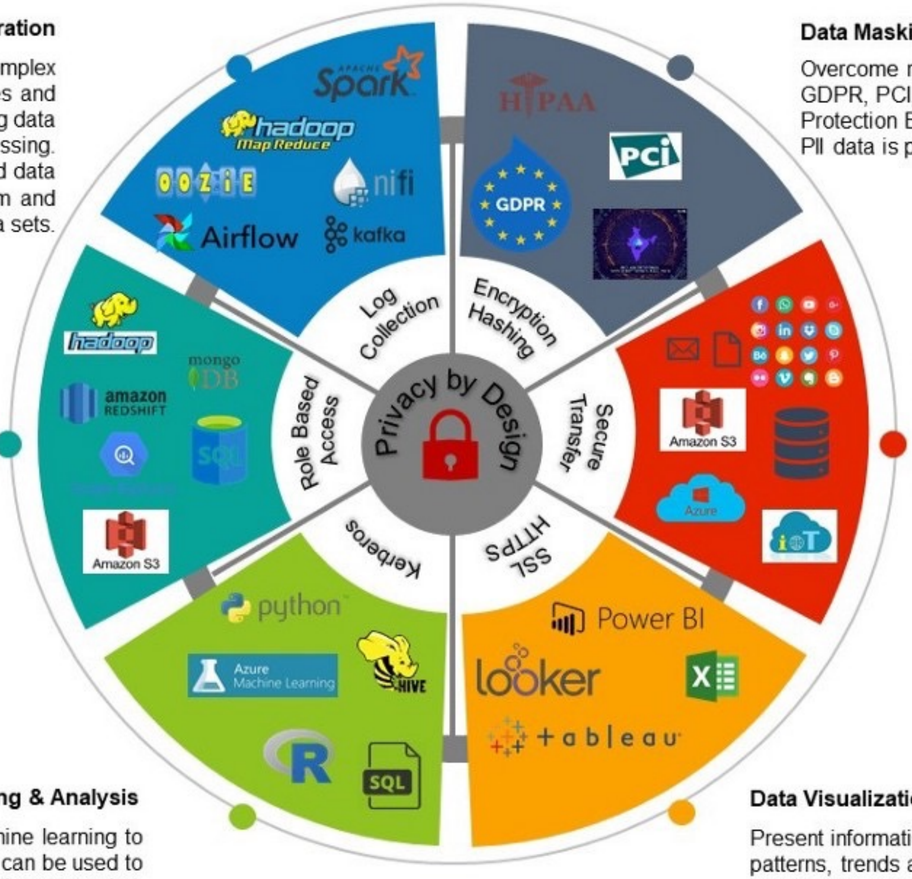
- Le concept de **Privacy by Design** englobe donc celui de la protection par défaut.
- Le concept de **Privacy by Default** consiste à prendre les mesures techniques et organisationnelles, pour garantir que, par défaut, seules les données qui nécessaires à l'aune de la finalité spécifique du traitement sont traitées. En clair, il faut régler les paramètres par défaut sur le mode le plus protecteur de la vie privée, l'utilisateur demeurant libre de les modifier. Exemple: opt-in, soit la possibilité de s'abonner à une newsletter.

Comme la majorité des violations légales ne sont pas détectées, mieux vaut donc empêcher leur survenance. Exemple (de Sylvain Métille) le formulaire papier à l'entrée du restaurant qui expose toutes les informations des précédents clients n'est pas conforme. Le recours à des fiches individuelles l'est.

< Fondements >

- Exemples:
- Floutage automatique des fenêtres ou des visages lors de l'utilisation d'un drone
- Loi sur la base de données référentielles et sur l'harmonisation des registres des personnes, des entreprises et établissements ainsi que des bâtiments et logements adoptée par le Canton du Valais (RS 172.8)
- Compteurs d'eau, cf. arrêt du Tribunal fédéral 1C_273/2020 destiné à publication:
  la mise en place de compteurs intelligents et plus généralement du « comptage intelligent » (« smart metering ») nécessite une véritable réflexion de la part des autorités quant au respect de la vie privée. Celle-ci doit intervenir à un stade précoce et donc dans le processus légistique d'élaboration des règles de droit, afin de tenir compte des normes relatives à la protection des données personnelles. En quelque sorte, le législateur et plus généralement les autorités doivent également prendre en compte le principe privacy by design dans l'action étatique. Kastriot Lubishtani

< Fondements >



Data Transformation & Orchestration

Join large data sets, apply complex transformations, apply data mapping rules and change data types suitable for big data processing.
Create automated pipelines that read data stored in batch or streaming, transform and rewrite final data sets.

Data Masking/De-identification

Overcome regulatory challenges such as GDPR, PCI, Indian Personal Data Protection Bill and HIPAA by ensuring that PII data is properly encrypted or masked.

Data Stores

Write transformed data sets to data lakes, data warehouses or cloud data stores.

Data Collection

Identify data points across the infrastructure. Data points can range from databases, raw files, social networking data, emails and IoT access points.

Data Modelling & Analysis

Dive deeper into your data using machine learning to develop models, These models can be used to maximize customer retention, reduce time to market, and boost market share.

Data Visualization

Present information in a graphic format to view patterns, trends and correlations using data visualization software.

Source: Manoj Kukreja, The Story of Data – Privacy by Design: https://towardsdatascience.com/the-story-of-data-privacy-by-design-530f4bfdfd8f

< Fondements >

- Mesures préventives, pas forcément compliquées à mettre en œuvre
- Obligation qui n’est pas absolue (pesée des intérêts en présence)
- Il ne s’agit pas d’empêcher le traitement des données, mais de le concilier avec des garde-fous
- Ces garanties (Privacy by Design & Privacy by default) doivent également être mises en œuvre lors de transferts de données, notamment vers des pays qui ne disposent pas de décision d’adéquation (CH en attente)
- Il s’agit d’obligations sous-tendant le principe de sécurité des données
- Différents outils permettent de démontrer le respect de ces obligations (registre des traitements et analyse d’impact notamment)

< Normes applicables : RGPD & LPD >

- Application (extraterritoriale) du RGPD à la Suisse, cf. Préposé fédéral à la protection des données et à la transparence, Le RGPD et ses conséquences sur la Suisse, état : mars 2018
- Pas d'application systématique aux résidents européens, aux travailleurs frontaliers et aux citoyens européens, ou la non-application aux administrations publiques suisses.
- Risque principal lié au suivi du comportement (3§2 RGPD).
- Les lignes directrices relatives à l'application territoriale tendent à assurer un haut niveau de protection des données dans le monde entier (Lignes directrices 3/2018 relatives au champ d'application territorial du RGPD (article 3), Version 2.0, 12 novembre 2019). Cf. Royal Courts of Justice, 15/01/2021

< Normes applicables : RGPD & LPD >

Art. 25: Protection des données dès la conception et protection des données par défaut [consid. 78]

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.

< Normes applicables : RGPD & LPD >

2. Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.
3. Un mécanisme de certification approuvé en vertu de l'article 42 peut servir d'élément pour démontrer le respect des exigences énoncées aux paragraphes 1 et 2 du présent article.

< Normes applicables : RGPD & LPD >

Le principe de Privacy by Design «vise à s'assurer que les responsables du traitement et les sous-traitants sont en mesure de s'acquitter des obligations qui leur incombent. Ce principe devrait également trouver application dans le cadre des marchés publics» §78 RGPD.

Les responsables du traitement et les sous-traitants ont une obligation de moyen renforcée en matière de sécurité des données. Pour démontrer le respect du RGPD, ils doivent adopter des règles internes et mettre en œuvre des mesures qui respectent les principes de PBDesign et PBDefault. Exemples: recours à la technique de pseudonymisation, minimisation des données, etc.

Le principe de PBDefault est régi par l'article 25 al. 2 RGPD. Il s'agit de la concrétisation du principe de minimisation des données. L'utilisateur est libre de réduire la protection de ses données en ayant accès à son compte.

< Normes applicables : RGPD & LPD >

Art. 7 Protection des données dès la conception et par défaut

1. Le responsable du traitement est tenu de mettre en place des mesures techniques et organisationnelles afin que le traitement respecte les prescriptions de protection des données, en particulier les principes fixés à l'art. 6 (principes). Il le fait dès la conception du traitement.
2. Les mesures techniques et organisationnelles doivent être appropriées au regard notamment de l'état de la technique, du type de traitement et de son étendue, ainsi que du risque que le traitement des données présente pour la personnalité ou les droits fondamentaux des personnes concernées.
3. Le responsable du traitement est tenu de garantir, par le biais de préréglages appropriés, que le traitement des données personnelles soit limité au minimum requis par la finalité poursuivie, pour autant que la personne concernée n'en dispose pas autrement.

< Normes applicables : RGPD & LPD >

Selon le message (FF 2017 6648 à 6650), l'alinéa 1er impose au responsable du traitement (de fait cela s'impose aussi aux fabricants de produits, aux prestataires de service et aux développeurs d'application, notamment; plus les mesures adéquates sont prises tôt, plus il est facile d'assurer la conformité du traitement) de concevoir dès l'origine le traitement dans le respect des normes en matière de protection des données. La protection technique des données personnelles ne s'appuie pas sur une technologie précise; elle passe plutôt par la mise en place de règles techniques et organisationnelles conformes aux principes définis à l'art. 6 nLPD. Les exigences légales doivent être intégrées ab ovo dans le système, de manière à rendre impossible une violation de la protection des données ou d'en réduire la probabilité. Exemples: fixation d'échéances régulières pour l'effacement ou l'anonymisation systématique; minimisation des données et fixation avant le début du traitement et contrôle de la durée de conservation à ce stade déjà.

< Normes applicables : RGPD & LPD >

Selon le message, l'alinéa 2 relatif aux mesures appropriées, la disposition se réfère au traitement de données effectué par des acteurs privés et par des organes fédéraux, d'où l'évocation des risques pesant sur la personnalité et sur les droits fondamentaux.

La norme matérialise l'approche fondée sur les risques. Il faut établir un rapport entre le risque induit par le traitement et les moyens techniques permettant de le réduire. Plus le risque est élevé, plus sa survenue est probable, et plus le traitement de données est important, plus les exigences auxquelles doivent répondre les mesures techniques pour être considérées comme appropriées au sens de cette disposition seront élevées.

Le message ne comporte aucun exemple de mesures techniques et organisationnelles appropriées. Il est souhaitable que l'Ordonnance (en cours de rédaction) pallie à ce manque et que le PFPDT publie un guide à l'instar du Comité Européen à la Protection des données.

< Normes applicables : RGPD & LPD >

L’une des questions qui se posent a trait au fait de savoir s’il convient d’adopter la mesure la plus stricte. Cela va dépendre du risque généré pour les personnes concernées par le traitement de données. Le principe de précaution est un fil conducteur intéressant.

Il faut combiner des mesures qui relèvent de la technologie et celles qui ne recourent pas à des systèmes informatiques (formation des collaborateurs).

Le principe de protection par défaut se matérialise par l’obligation d’effectuer une AIPD (analyse d’impact relative à la protection des données), dans certaines circonstances (cf. art. 22 nLPD). Une AIPD est obligatoire lorsque le traitement de données est susceptible d’entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Des exceptions sont prévues (système, produit, service certifié / respect d’un code de conduite).

< Normes applicables : RGPD & LPD >

L’alinéa 3 concerne la protection des données par défaut.

Le message précise que les mesures en question résident dans des réglages prédéfinis (ex: installation d’un logiciel), qui s’appliquent de manière standardisée, lorsque l’utilisateur ne choisit pas une autre voie.

Ces paramètres standards peuvent être effectués en usine ou ultérieurement (par ex. définir, pour un ordinateur, une imprimante par défaut). Le processus de traitement doit être préprogrammé de manière à garantir autant que possible la protection des données. La personne concernée peut toutefois en modifier les paramètres. Certains sites Internet autorisent par principe les achats sans qu’il faille créer un profil d’utilisateur. Les clients ne fournissent que des informations minimales, soit leur nom et l’adresse de livraison. Ceux qui souhaitent bénéficier de services supplémentaires, tels que l’accès à leur historique d’achat ou à des offres ou la création d’une liste de shopping, doivent consentir à un traitement plus complet de leurs données.

< Normes applicables : RGPD & LPD >

Le lien avec la protection des données dès la conception est étroit. En effet, ces réglages prédéfinis s’inscrivent souvent dans un système entier respectueux de la protection des données. Ce qui est spécifique, c’est l’influence éventuelle de la personne concernée. Alors qu’elle ne peut en principe pas modifier le système lui-même, elle a toujours la possibilité, s’agissant des réglages par défaut, de choisir une solution différente et donc de consentir à un traitement déterminé.

La protection des données par défaut joue un rôle mineur dans le secteur public, car les traitements y reposent moins sur le consentement de la personne concernée que sur des obligations légales.

Le responsable du traitement peut démontrer, par une certification ou une analyse d’impact relative à la protection des données notamment, qu’il respecte les obligations définies dans cette disposition.

< Discrépances : RGPD & LPD >

Quelles sont, selon vous, les principales différences
entre le régime juridique prévu par le RGPD et celui prévu par la LPD?

1. Initialement la sanction prévue par la nLPD était de CHF 500’000.- (acte intentionnel) ou CHF 250’000.-(négligence); elle a été abandonnée; par contre possibilité de prononcer une sanction pénale si le responsable du traitement viole intentionnellement le devoir d’informer ou faillit à son devoir de diligence (par ex. en violant les normes sur les transferts de données à l’étranger, de sécurité des données ou de sous-traitance). Action civile réservée (art. 28 ss CC).

2. Amende administrative selon le RGPD pouvant s’élever à 10 millions ou pour les entreprises jusqu’à 2% du CA annuel mondial de l’exercice précédent, le montant le plus élevé étant retenu.

< Conclusion >

Aucun délai transitoire n’est prévu par la nLPD.

L’obligation de protection dès la conception ne s’appliquera pas rétroactivement aux traitements de données effectués avant l’entrée en vigueur de la nLPD, pour autant que les finalités du traitement demeurent inchangées et que de nouvelles données ne soient pas collectées (art. 69 nLPD).

Les cas où les traitements de données demeurent inchangés sont relativement rares. Au demeurant de nouvelles (autres) obligations devront être implémentées.

Il convient dès lors d’agir avec célérité pour la mise en conformité globale.

Suivi des décisions en matière de GDPR

GDPR Enforcement Tracker

tracked by CMS Law.Tax

The CMS.Law GDPR Enforcement Tracker is an overview of fines and penalties which data protection authorities within the EU have imposed under the EU General Data Protection Regulation (GDPR, DSGVO). Our aim is to keep this list as up-to-date as possible. Since not all fines are made public, this list can of course never be complete, which is why we appreciate any indication of further GDPR fines and penalties. *Please note that we do not list any fines imposed under national / non-European laws, under non-data protection laws (e.g. competition laws / electronic communication laws) and under "old" pre-GDPR-laws.*

New features: "ETid" and "Direct URL"!
We have assigned a unique and permanent ID to each fine in our database, which makes it possible to precisely address fines, e.g. in publications. Once an "ETid" has been assigned to a fine, it remains the same, even if the fine is overturned or amended by courts at a later date, or if we add fines that were issued chronologically before. The "Direct URL" (click "+" or on a specific ETid to view details of a fine) can be used to share fines online, e.g. on Twitter or other media.

Show 10 entries

Search:

ETid	Country	Date	Fine [€]	Controller/Processor	Quoted Art.	Type	Source
ETid-564	POLAND	2021-02-11	22,200	Krajowa Szkoła Sądownictwa i Prokuratury	Art. 5 (1) f) GDPR, Art. 25 (1) GDPR, Art. 28 (3) GDPR, Art. 32 (1), (2) GDPR	Insufficient technical and organisational measures to ensure information security	link
ETid-537	BELGIUM	2021-01-27	50,000	Family Service / N.D.P.K. nv.	Art. 5 GDPR, Art. 6 GDPR, Art. 7 GDPR, Art. 13 GDPR, Art. 24 GDPR, Art. 25 GDPR, Art. 28 GDPR	Insufficient legal basis for data processing	link
ETid-509	POLAND	2020-12-17	235,300	ID Finance Poland Sp. z o.o.	Art. 5 (1) f) GDPR, Art. 25 (1) GDPR, Art. 32 (1) b), d), (2) GDPR	Insufficient technical and organisational measures to ensure information security	link
ETid-494	HUNGARY	2020-12-16	55,400	Robinson Tours Ltd. (Robinson Tours Idegenforgalmi és Szolgáltató Kft.)	Art. 25 (1), (2) GDPR, Art. 32 (1) b) GDPR, Art. 34 (1) GDPR	Insufficient technical and organisational measures to ensure information security	link
ETid-483	POLAND	2020-12-14	443,000	Virgin Mobile Polska	Art. 5 (1) f), (2) GDPR, Art. 25 (1) GDPR, Art. 32 (1) b), d), (2) GDPR	Insufficient technical and organisational measures to ensure information security	link
ETid-460	BELGIUM	2020-11-25	1,500	Private Individual	Art. 6 GDPR, Art. 25 GDPR	Insufficient legal basis for data processing	link
ETid-438	ITALY	2020-11-12	12,251,601	Vodafone Italia S.p.A.	Art. 5 (1), (2) GDPR, Art. 6 (1) GDPR, Art. 7 GDPR, Art. 15 (1) GDPR, Art. 16 GDPR, Art. 21 GDPR, Art. 24 GDPR, Art. 25 (1) GDPR, Art. 32 GDPR, Art. 33 GDPR	Non-compliance with general data processing principles	link
ETid-430	HUNGARY	2020-10-23	54,800	Deichmann Cipőkereskedelmi Korlátolt Felelősségű Társaságnak	Art. 12 GDPR, Art. 15 GDPR, Art. 18 (1) c) GDPR, Art. 25 GDPR	Insufficient fulfilment of data subjects rights	link
ETid-395	ROMANIA	2020-09-01	500	Apartment building owners association	Art. 5 GDPR, Art. 6 GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 25 GDPR, Art. 32 GDPR	Insufficient legal basis for data processing	link
ETid-336	ITALY	2020-07-13	16,700,000	Wind Tre S.p.A.	Art. 5 GDPR, Art. 6 GDPR, Art. 12 GDPR, Art. 24 GDPR, Art. 25 GDPR	Insufficient legal basis for data processing	link

Suivi des décisions en matière de LPD

LPD DSG Suivi d'application Suisse

suivi par LEXING SWITZERLAND

Filtrer par canton:

- VS
- VD

Filtrer par violation (art.):

- 3
- 32

Effacer les filtres

Afficher 10 éléments

Rechercher :

Réf.	Ré...	Date	Amende	Maître	Art. cité	Autorité	Secteur	Résumé	Lien direct
3443	VS	24/04/2021	CHF 2590	Mr. Branche	3	Justice Vaudoise	Automob...	résumé en texte....	
7553	VD	14/04/2021	CHF 2000	Mr. Guy G.	32	Justice Valaisanne	Vente en ligne	Texte de résumé..	

www.lpd-dsg.ch

Conseils

- nommer un DPO ;
- vérifier et adapter les déclarations de protection des données aux nouvelles exigences ;
- établir un registre des traitements de données personnelles ;
- vérifier et adapter les contrats de sous-traitance ;
- identifier les transferts de données vers l'étranger, et vérifier s'ils répondent aux nouvelles conditions ;
- préparer un processus d'analyse d'impact ;
- préparer un processus de détection et d'annonce des violations de données ;
- préparer ou mettre à jour les processus de traitement des demandes des personnes concernées (droit d'accès, rectification, droit à l'oubli, etc.).

Sébastien Fanti - CV

- Licence en droit (Master) utriusque juris de l'Université de Fribourg
- Avocat au Barreau valaisan, Notaire et fondateur du réseau Lexing
- Conseiller en protection des données HEIG-VD (2014)
- Information Security Lead Auditor ISO 27001 :2013 (2015)
- Security Management Lead Implementer ISO 27001 :2013 (2015)
- Certified Lead Privacy Implementer ISO 29100 (2015)
- Chargé de cours à l'Université Pierre et Marie Curie (UPMC) – la Sorbonne : DE Data Strategist, Paris (depuis 2017)
- Élu Préposé à la protection des données et à la transparence du Canton du Valais (2015 – 2022)
- Certified Information Privacy Professional / Europe (2018)
- Auditeur RGPD certifié Bureau Veritas (2019)
- CAS Digital Finance Law UNIGE (2020)

LEXING

SWITZERLAND

Obedient to Your interest

www.twitter.com/**sebastienfanti**

www.facebook.com/**sebastien.fanti**

ch.linkedin.com/in/**sebastienfanti**

sebastien.fanti@sebastienfanti.ch

LSFin

Sion, mercredi 28 avril 2021

Yann R. CORBAZ – Lexing Switzerland Sàrl

Avant-propos

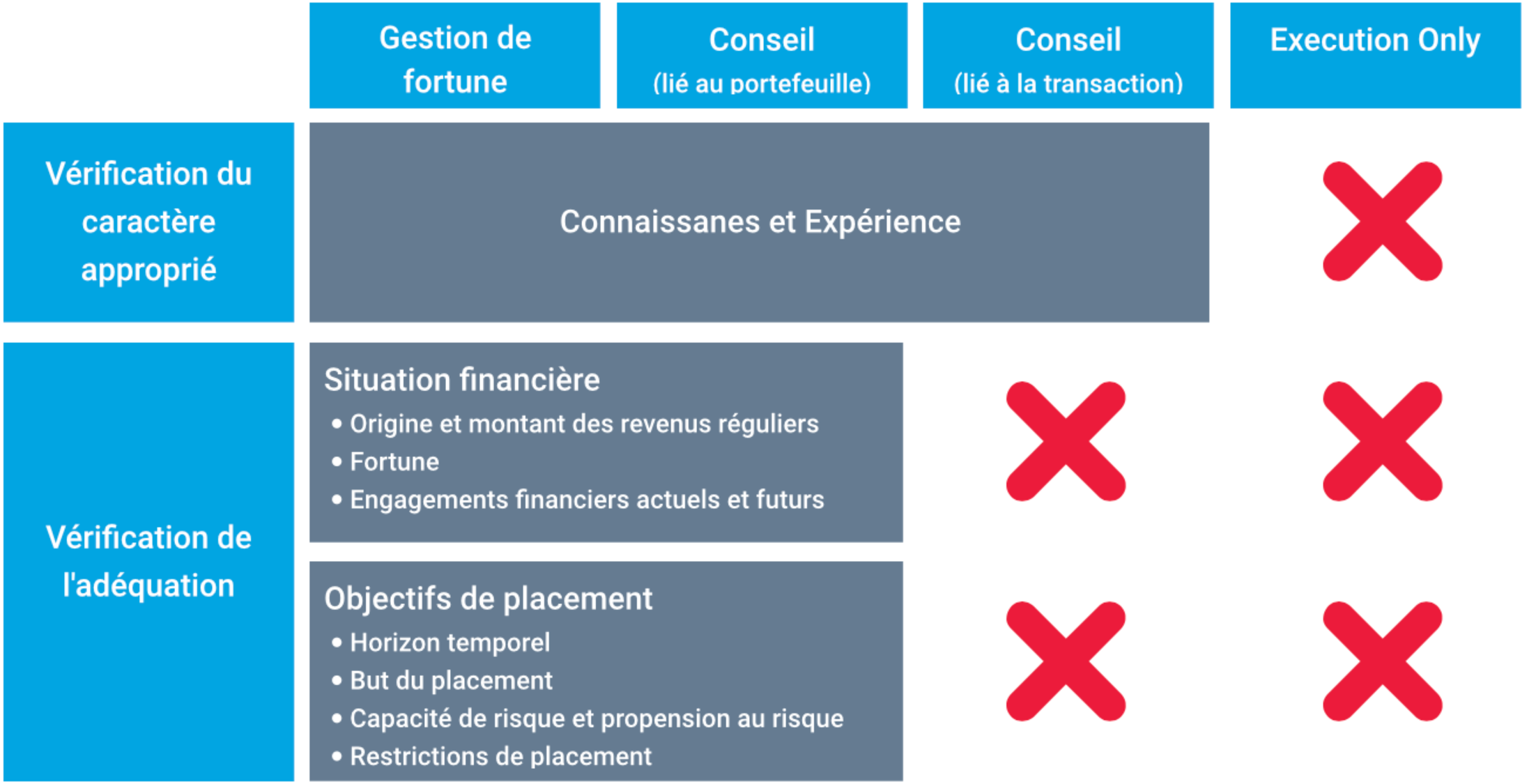
***Accounting Dpt.* dans les banques : un rôle essentiel**

Finance -> Accounting
Etablissement des comptes – Liens avec les auditeurs internes et externes - FINMA
ISDA: Netting (complexe) - Treasury & Trading/ CFO/ COO
Rapports FINMA - notamment LCR (Liquidity Coverage Ratio -> short-term obligations)
Calcul des éventuelles rétrocessions, év. crédits etc.
Préparation des rapports annuels

LSFin

- La Loi fédérale sur les services financiers (LSFin) est entrée en vigueur en janvier 2020. Étant donné la période de transition de deux ans qu'elle prévoit, la plupart de ses dispositions prendront effet à compter de janvier 2022.

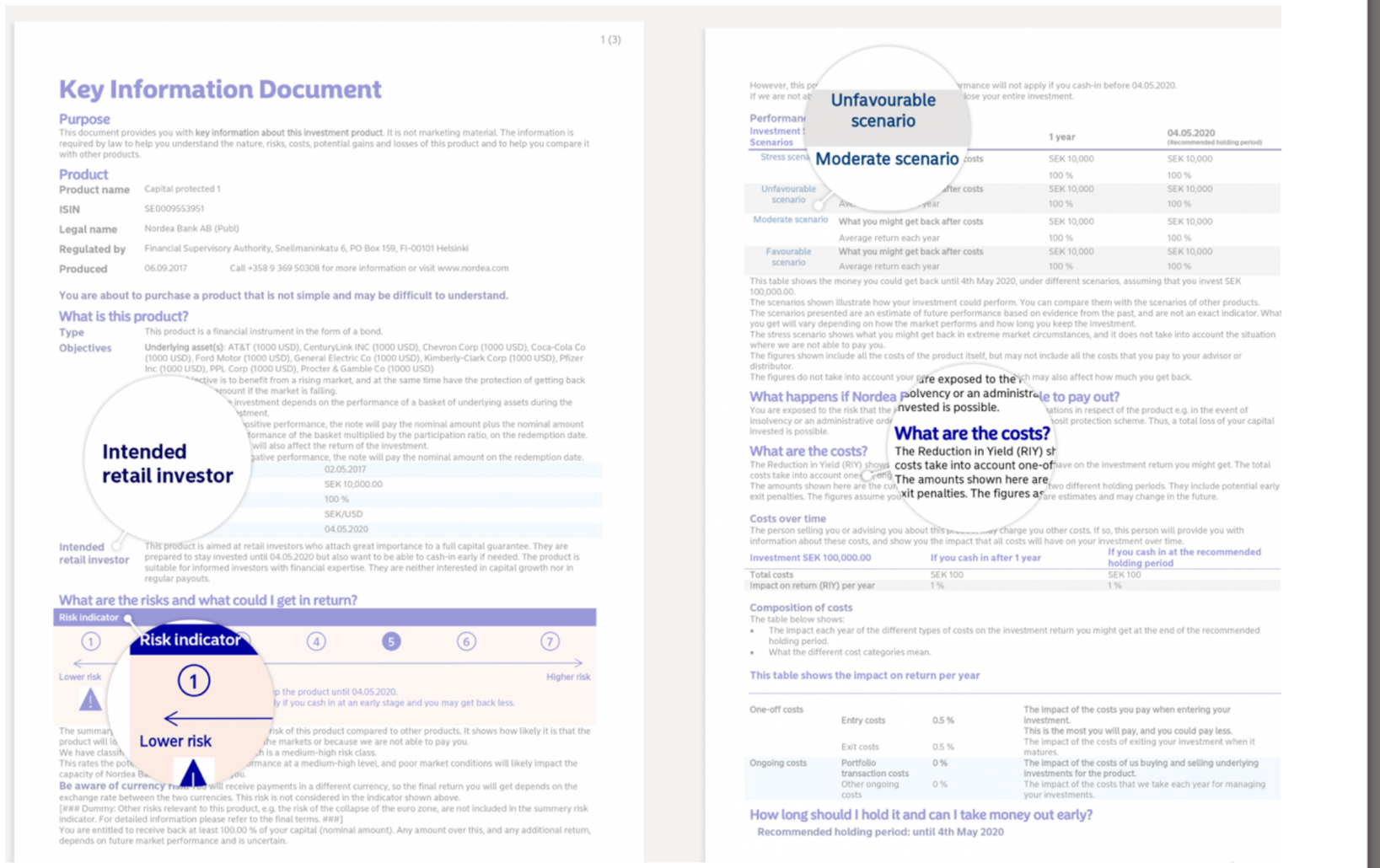
- La loi sur les services financiers (LSFin) vise à renforcer la protection des investisseurs et à établir des normes comparables pour les fournisseurs de services financiers. Elle exige de ces derniers qu’ils adoptent des règles de conduite plus strictes et qu’ils fournissent à leurs clients des informations et une documentation complète.


Gestion de fortune
Conseil (lié au portefeuille)
Conseil (lié à la transaction)
Execution Only
Vérification du caractère approprié
Connaissanes et Expérience
Vérification de l'adéquation
Situation financière
• Origine et montant des revenus réguliers
• Fortune
• Engagements financiers actuels et futurs
Objectifs de placement
• Horizon temporel
• But du placement
• Capacité de risque et propension au risque
• Restrictions de placement

Source: BDO

Coûts pour les prestataires de services financiers

- Art. 8 al. 2 LSFin :
- (Les prestataires de services financiers) informent (les clients) en outre:
- a. du service financier qui fait l'objet de la recommandation personnalisée et des risques et coûts y afférents;
- b. de leurs relations économiques avec des tiers concernant les services financiers proposés;
- c. de l'offre du marché prise en considération pour la sélection des instruments financiers.
- [3] Si la recommandation personnalisée porte sur des instruments financiers, les prestataires de services financiers mettent en sus à la disposition de leurs clients privés la feuille d'information de base, lorsque celle-ci doit être établie pour l'instrument financier recommandé (art. 58 et 59). Si l'instrument financier recommandé est un instrument financier composé, une feuille d'information de base doit être mise à disposition uniquement pour ce dernier.
- [4] Aucune feuille d'information de base ne doit être mise à disposition lorsque les services se limitent à l'exécution ou à la transmission d'ordres des clients, sauf lorsqu'une feuille d'information de base existe déjà pour l'instrument financier.
- [5] Si la recommandation personnalisée porte sur des instruments financiers pour lesquels un prospectus doit être établi (art. 35 à 37), les prestataires de services financiers mettent gratuitement le prospectus à la disposition de leurs clients privés lorsque ceux-ci le demandent.



1 (3)

Key Information Document

Purpose

This document provides you with **key information about this investment product**. It is not marketing material. The information is required by law to help you understand the nature, risks, costs, potential gains and losses of this product and to help you compare it with other products.

Product

Product name	Capital protected 1
ISIN	SE0009553951
Legal name	Nordea Bank AB (Publ)
Regulated by	Financial Supervisory Authority, Snellmaninkatu 6, PO Box 159, FI-00101 Helsinki
Produced	06.09.2017 Call +358 9 369 50308 for more information or visit www.nordea.com

You are about to purchase a product that is not simple and may be difficult to understand.

What is this product?

Type This product is a financial instrument in the form of a bond.

Objectives **Underlying asset(s)**: AT&T (1000 USD), CenturyLink INC (1000 USD), Chevron Corp (1000 USD), Coca-Cola Co (1000 USD), Ford Motor (1000 USD), General Electric Co (1000 USD), Kimberly-Clark Corp (1000 USD), Pfizer Inc (1000 USD), PPL Corp (1000 USD), Procter & Gamble Co (1000 USD)

...ective is to benefit from a rising market, and at the same time have the protection of getting back ...mount if the market is falling.

... investment depends on the performance of a basket of underlying assets during the ...stment.

...positive performance, the note will pay the nominal amount plus the nominal amount ...formance of the basket multiplied by the participation ratio, on the redemption date. ... will also affect the return of the investment.

...gative performance, the note will pay the nominal amount on the redemption date.

	02.05.2017
	SEK 10,000.00
	100 %
	SEK/USD
	04.05.2020

Intended retail investor This product is aimed at retail investors who attach great importance to a full capital guarantee. They are prepared to stay invested until 04.05.2020 but also want to be able to cash-in early if needed. The product is suitable for informed investors with financial expertise. They are neither interested in capital growth nor in regular payouts.

What are the risks and what could I get in return?

Risk indicator

1 2 3 4 5 6 7

Lower risk Higher risk

...p the product until 04.05.2020.

...y if you cash in at an early stage and you may get back less.

The summar... ...risk of this product compared to other products. It shows how likely it is that the product will lo... ...the markets or because we are not able to pay you.

We have classifi... ...h is a medium-high risk class.

This rates the pot... ...ormance at a medium-high level, and poor market conditions will likely impact the capacity of Nordea Ba... ...ou.

Be aware of currency risk. You will receive payments in a different currency, so the final return you will get depends on the exchange rate between the two currencies. This risk is not considered in the indicator shown above.

[### Dummy: Other risks relevant to this product, e.g. the risk of the collapse of the euro zone, are not included in the summery risk indicator. For detailed information please refer to the final terms. ###]

You are entitled to receive back at least 100.00 % of your capital (nominal amount). Any amount over this, and any additional return, depends on future market performance and is uncertain.

However, this pr... ...rmance will not apply if you cash-in before 04.05.2020.

If we are not ab... ...ose your entire investment.

Performan...

Investment ... Scenarios		1 year	04.05.2020 (Recommended holding period)
Stress scena...	...costs	SEK 10,000	SEK 10,000
		100 %	100 %
Unfavourable scenario	...fter costs	SEK 10,000	SEK 10,000
	Av... ...year	100 %	100 %
Moderate scenario	What you might get back after costs	SEK 10,000	SEK 10,000
	Average return each year	100 %	100 %
Favourable scenario	What you might get back after costs	SEK 10,000	SEK 10,000
	Average return each year	100 %	100 %

This table shows the money you could get back until 4th May 2020, under different scenarios, assuming that you invest SEK 100,000.00.

The scenarios shown illustrate how your investment could perform. You can compare them with the scenarios of other products.

The scenarios presented are an estimate of future performance based on evidence from the past, and are not an exact indicator. What you get will vary depending on how the market performs and how long you keep the investment.

The stress scenario shows what you might get back in extreme market circumstances, and it does not take into account the situation where we are not able to pay you.

The figures shown include all the costs of the product itself, but may not include all the costs that you pay to your advisor or distributor.

The figures do not take into account your ...ax ...ich may also affect how much you get back.

What happens if Nordea P... ...le to pay out?

You are exposed to the risk that the ... ...ations in respect of the product e.g. in the event of insolvency or an administrative ord... ...posit protection scheme. Thus, a total loss of your capital invested is possible.

What are the costs?

The Reduction in Yield (RIY) shows ... ...have on the investment return you might get. The total costs take into account one-... ...end ... The amounts shown here are the cu... ...two different holding periods. They include potential early exit penalties. The figures assume you ... ...re estimates and may change in the future.

Costs over time

The person selling you or advising you about this p... ...y charge you other costs. If so, this person will provide you with information about these costs, and show you the impact that all costs will have on your investment over time.

Investment SEK 100,000.00	If you cash in after 1 year	If you cash in at the recommended holding period
Total costs	SEK 100	SEK 100
Impact on return (RIY) per year	1 %	1 %

Composition of costs

The table below shows:

- The impact each year of the different types of costs on the investment return you might get at the end of the recommended holding period.
- What the different cost categories mean.

This table shows the impact on return per year

One-off costs	Entry costs	0.5 %	The impact of the costs you pay when entering your investment. This is the most you will pay, and you could pay less.
	Exit costs	0.5 %	The impact of the costs of exiting your investment when it matures.
Ongoing costs	Portfolio transaction costs	0 %	The impact of the costs of us buying and selling underlying investments for the product.
	Other ongoing costs	0 %	The impact of the costs that we take each year for managing your investments.

How long should I hold it and can I take money out early?

Recommended holding period: until 4th May 2020

Intended retail investor

Unfavourable scenario

Moderate scenario

What are the costs?

The Reduction in Yield (RIY) sh... costs take into account one-of... The amounts shown here are... ...xit penalties. The figures as...

Risk indicator

1

Lower risk

Europe – Mifid II/ *PRIIPS-KID*

Impacts sur les Circulaires FINMA

1 **Circulaire FINMA 2008/14 « Reporting prudentiel – banques » du 20 novembre 2008**

2 **Circulaire FINMA 2013/3 « Activités d'audit » du 6 décembre 2012**

- 2.1 Annexe 2 « Stratégie d'audit standard – banques / maisons de titres »
- 2.2 Annexe 13 « Analyse des risques – banques / maisons de titres »
- 2.3 Annexe 16 « Analyse des risques Infrastructures des marchés financiers » et annexe 17 « Stratégie d'audit standard Infrastructures des marchés financiers »
- 2.4 Annexe 19 « Indications complémentaires fournies dans le rapport sur l'audit comptable des assurances »

3 **Circulaire FINMA 2013/8 « Règles de conduite sur le marché » du 29 août 2013**

4 **Circulaire FINMA 2015/2 « Risque de liquidité – banques » du 3 juillet 2014**

5 **Circulaire FINMA 2017/7 « Risques de crédit – banques » du 7 décembre 2016**

6 **Circulaire FINMA 2018/3 « *Outsourcing* » du 21 septembre 2017**

7 **Circulaire FINMA 2020/1 « Comptabilité – banques » du 31 octobre 2019 - annexe 1 « Détails relatifs aux postes du bilan et aux opérations hors bilan »**

8 **Circulaires abrogées**

RETROCESSION Arrêt TF 4A_355/2019 du 13 mai 2020

- “[La] rémunération sur la masse détenue en fonds de placement, produits structurés, autres produits bancaires ou sur les apports effectués par le client se situe dans une fourchette allant de 0 % à 1 % du volume investi”. *PAS SUFFISEMMENT PRECIS*

Droit du mandat (initial). La LSFin retranscrit en droit administratif les principes de droit civil dégagés par le Tribunal fédéral. Art. 26 LSFin et 29 OSFin applicable aux mandat de gestion, de conseil en placement et aux relations d’*execution only*.

Problème de conflits d’intérêts

- Dépôts d’assets dans une banque avec rétrocessions. Même en cas de meilleur tarif ! (ATF)

Attention corruption active et passive privée 322octies et novies CP !

- Attention MIFID II: (activité irréprochable)

Divers

Fin 2021 fin du LIBOR (CH : SARON)

Adaptation/ nouveaux contrats ISDA entre les banques

Anecdotes *Custodian banks*

Merci pour votre attention !

COMPTAVAL
ASSOCIATION VALAISANNE DES EXPERTS EN FINANCE ET CONTROLLING ET SPECIALISTES EN FINANCE ET COMPTABILITE

Mercredi 28 avril 2021 à 17h00, en direct de Sion