

ROYAUME DE BELGIQUE	KONINKRIJK BELGIE
Service public fédéral Justice et Finances	Federale Overheidsdienst Justitie en Financiën
Avant-projet de loi portant création d'un système d'alerte d'incidents dans le secteur financier	Voorontwerp van wet houdende de oprichting van een incidentenwaarschuwingssysteem binnen de financiële sector
PHILIPPE, Roi des Belges,	FILIP, Koning der Belgen,
A tous, présents et à venir, Salut.	Aan allen die nu zijn en hierna wezen zullen, Onze Groet.
Sur la proposition du Ministre de la Justice et du Ministre des Finances,	Op de voordracht van de Minister van Justitie en de Minister van Financiën,
NOUS AVONS ARRETE ET ARRETONS :	HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ:
Le Ministre de la Justice et le Ministre des Finances sont chargés de présenter en notre nom à la Chambre des représentants le projet de loi dont la teneur suit :	De Minister van Justitie et de Minister van Financiën zijn ermee belast in onze naam bij de Kamer van volksvertegenwoordigers het ontwerp van wet in te dienen waarvan de tekst hierna volgt:
Section 1^{re}. Dispositions générales	Afdeling 1. Algemene bepalingen
Article 1^{er}. Fondement constitutionnel	Artikel 1. Grondwettelijke grondslag
La présente loi règle une matière visée à l'article 74 de la Constitution.	Deze wet regelt een aangelegenheid zoals bedoeld in artikel 74 van de Grondwet.
Article 2. Définitions	Artikel 2. Definities
Pour l'application de la présente loi, on entend par :	Voor de toepassing van deze wet wordt verstaan onder:
1° « système » : le système d'alertes d'incidents tel que créé par la présente loi ;	1° "het systeem": het systeem van incidentenwaarschuwingen zoals opgericht door deze wet;
2° « incident » : un incident tel que défini à l'article 5, § 1 ^{er} ;	2° "het incident": een incident zoals gedefinieerd in artikel 5, § 1;
3° « données d'incidents » : les données collectées et gérées directement par chaque établissement concerné individuellement dans	3° "de incidentengegevens": de gegevens die door elke individuele betrokken instelling rechtsreeks verzameld en beheerd worden in

le cadre d'un incident qui se produit dans l'établissement concerné ;

4° « données d'alerte » : les données enregistrées dans le registre d'alerte ;

5° « le registre d'alerte » : le registre contenant les données décrites à l'article 6 de la présente loi, lesquelles sont échangées de manière structurelle par les établissements concernés.

6° « établissement concerné » :

a) les établissements de crédit visés à l'article 1^{er}, § 3, alinéa 1^{er}, de la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse, qui relèvent du droit belge ;

b) les succursales en Belgique d'établissements de crédit visés à l'article 1^{er}, § 3, alinéa 1^{er}, de la loi précitée, qui relèvent du droit d'un autre État membre de l'Espace économique européen ou d'un pays tiers ;

c) les établissements de crédit visés à l'article 1^{er}, § 3, alinéa 1^{er}, de la même loi, qui relèvent du droit d'un autre État membre de l'Espace économique européen et qui font appel à un agent établi en Belgique pour y fournir des services qui consistent en la réception de dépôts ou d'autres fonds remboursables, au sens de l'article 4, 1), de la loi précitée ;

d) les prêteurs au sens de l'article I.9, 34°, du Code de droit économique qui sont établis en Belgique et qui exercent des activités de crédit à la consommation ou de crédit hypothécaire, conformément au livre VII, titre 4, chapitres 1^{er} et 2, du même Code, ainsi que les succursales en Belgique de personnes exerçant des activités équivalentes relevant du droit d'un autre État membre de l'Espace économique européen ;

het kader van een incident dat zich bij de betrokken instelling voordoet;

4° “de waarschuwingsgegevens” : de gegevens die opgenomen zijn in het waarschuwingsregister;

5° “het waarschuwingsregister” : het register dat de door artikel 6 van deze wet beschreven gegevens bevat, welke gegevens door de betrokken instellingen op structurele manier met elkaar worden uitgewisseld;

6° “de betrokken instelling”:

a) de kredietinstellingen bedoeld in artikel 1, § 3, eerste lid, van de wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen en beursvennootschappen, die vallen onder het Belgische recht;

b) de in België gevestigde bijkantoren van kredietinstellingen als bedoeld in artikel 1, § 3, eerste lid, van voornoemde wet, die vallen onder het recht van een andere lidstaat van de Europese Economische Ruimte of van een derde land;

c) de kredietinstellingen bedoeld in artikel 1, § 3, eerste lid, van dezelfde wet, die vallen onder het recht van een andere lidstaat van de Europese Economische Ruimte en die een beroep doen op een in België gevestigde agent om er diensten te leveren die bestaan in het in ontvangst nemen van deposito's of andere terugbetaalbare gelden, in de zin van artikel 4, 1), van de voornoemde wet;

d) de kredietgevers in de zin van artikel I.9, 34°, van het Wetboek van economisch recht die in België gevestigd zijn en die activiteiten van consumentenkrediet of hypothecaire krediet uitoefenen, als bedoeld in boek VII, titel 4, hoofdstukken 1 en 2, van hetzelfde Wetboek, evenals de in België gevestigde bijkantoren van personen die gelijkwaardige werkzaamheden uitoefenen die vallen onder het recht van een andere lidstaat van de Europese Economische Ruimte.

7° « personne enregistrée » : la personne physique ou morale impliquée dans un incident tel que prévu par la loi, qui a manifesté des comportements ayant porté ou pouvant porter préjudice à l'établissement concerné, à ses clients et à l'intégrité du secteur financier et qui, après une enquête documentée, est enregistrée dans le système par la personne compétente de l'établissement concerné.

7° “de geregistreerde persoon”: is een natuurlijke of rechtspersoon die betrokken is in een incident zoals voorzien door de wet, die gedragingen heeft vertoond die hebben geleid of kunnen leiden tot de benadeling van de betrokken instelling, diens cliënten en de integriteit van de financiële sector en die na gedocumenteerd onderzoek door de bevoegde persoon van de betrokken instelling geregistreerd wordt in het systeem.

Section 2. Création du système d'alerte d'incidents

Afdeling 2. Oprichting van het Incidentenwaarschuwingssysteem

Article 3. But du système

Artikel 3. Doel van het systeem

La présente loi règle l'échange de données d'alerte par les établissements concernés en vue de lutter contre l'usage abusif des services de paiement et des crédits tels que définis par l'article 9.I.1° et l'article 9.I.39° du Code de Droit Economique et de l'article 2,3° de la loi du 21 décembre 2013 relative à diverses dispositions concernant le financement des petites et moyennes entreprises.

Deze wet regelt de uitwisseling van waarschuwingsgegevens door de betrokken instellingen met het oog op het bestrijden van het oneigenlijk gebruik van betalingsdiensten en kredieten zoals gedefinieerd in artikel 1.9.1° en artikel 1.9.39° Wetboek Economisch Recht en artikel 2,3° van de wet van 21 december 2013 betreffende diverse bepalingen inzake de financiering van kleine en middelgrote ondernemingen

Les données enregistrées dans le système et échangées au moyen de celui-ci servent exclusivement les finalités suivantes :

De gegevens opgeslagen in en uitgewisseld door middel van het systeem dienen uitsluitend de volgende doeleinden:

1° la prévention, la recherche et la détection d'incidents ;

1° het voorkomen van, het onderzoek naar en de opsporing van incidenten;

2° le partage de données entre les établissements concernés à propos d'incidents ;

2° het delen van gegevens tussen de betrokken instellingen met betrekking tot incidenten;

3° la protection des personnes physiques ou morales victimes d'incidents.

3° de bescherming van de natuurlijke personen of rechtspersonen die slachtoffer zijn van incidenten.

Article 4. Description du système

Les établissements concernés prévoient un système électronique d'alerte d'incident, appelé ci-après « le système ». Ce système est composé, d'une part, de données qui sont directement collectées et gérées au niveau des établissements concernés individuels dans le cadre d'un incident, à savoir les données d'incident, et, d'autre part, de données limitées, à savoir les données d'alerte, qui sont échangées par les établissements concernés de manière structurelle au moyen d'un registre d'alerte.

Artikel 4. Beschrijving van het systeem

De betrokken instellingen voorzien in een elektronisch systeem voor incidentenwaarschuwingen, hierna "het systeem" genaamd. Dit systeem bestaat enerzijds uit gegevens die op het niveau van de individuele betrokken instellingen rechtstreeks verzameld en beheerd worden in het kader van een incident, zijnde de incidentengegevens, en uit beperkte gegevens, zijnde de waarschuwingsgegevens, die door de betrokken instellingen op structurele manier met elkaar uitgewisseld worden via een waarschuwingsregister.

Section 3. Incidents et traitement

Afdeling 3. Incidenten en behandeling

Article 5. Incidents

Artikel 5. Incidenten

§ 1^{er}. Par incident, on entend :

§ 1. Onder incident wordt verstaan:

1° la commission ou la tentative de commission de faits au sens de l'article 6, 13°, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ;

1° het plegen of trachten te plegen van feiten in de zin van artikel 6, 13°, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;

2° la commission ou la tentative de commission d'actes pouvant donner lieu à des incidents de sécurité ou à des réclamations en lien avec la sécurité au sens de l'article 53 de la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement, et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement ;

2° het plegen of trachten te plegen van daden die aanleiding kunnen geven tot veiligheidsincidenten of veiligheidsgerelateerde klachten in de zin van artikel 53 van de wet van 11 maart 2018 betreffende het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld, en de toegang tot betalingssystemen;

3° la cybermenace au sens de l'article 2 (8) du Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le

3° cyberdreigingen in de zin van artikel 2 (8) van verordening EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van

Règlement (UE) n° 526/2013 (le « Règlement sur la cybersécurité ») ;

4° la production d'une facture dans laquelle des données ont été adaptées par une partie autre que la partie qui a établi la facture ;

5° les cas où une personne s'approprie l'identité ou la fonction d'une autre personne ou utilise des documents d'identité falsifiés ;

6° l'utilisation de documents falsifiés, comme des attestations de revenus et des justificatifs d'investissement, en vue de l'obtention d'un crédit ;

7° les cas où une personne persuade une autre par n'importe quelle technique de transférer et/ou de soustraire des données et/ou des fonds, en vue de l'abus de ces données ;

8° les cas où le compte bancaire d'une personne est utilisé pour recevoir et/ou transférer illicitement des fonds de tiers, dans le but de dissimuler l'identité de ce tiers.

9° les cas de fraude et de contrefaçon des moyens de paiement autres que les espèces au sens du projet de loi transposant la Directive 2019/713 du Parlement européen et du Conseil du 17 avril 2019 concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces et remplaçant la décision cadre 2001/413/JAI du Conseil.

Le Roi peut compléter les catégories d'incidents visés à l'alinéa 1^{er}.

§ 2. Les personnes compétentes désignées par l'établissement concerné conformément à l'article 9, alinéa 2, doivent toujours évaluer si un ou plusieurs des cas décrits au paragraphe 1^{er} sont rencontrés. En cas de doute, la décision de procéder ou non à l'enregistrement est prise au bénéfice de la personne liée à l'incident.

La décision ne peut pas conduire à l'enregistrement d'une personne lorsqu'il est

Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening);

4° voorleggen van een factuur waarin er gegevens werden aangepast door een partij andere dan de partij welke de factuur uitschreef;

5° gevallen waar een persoon zich de identiteit of functie van een andere persoon toe-eigent of gebruik maakt van vervalste identiteitsdocumenten;

6° het gebruik van vervalste stukken, zoals inkomstenbewijzen en investeringsbewijzen, met het oog op het verkrijgen van een krediet;

7° gevallen waarbij een persoon een ander via eender welke techniek overtuigt om gegevens en/of fondsen over te dragen en/of te onvreemden, met het oog op het misbruik van deze gegevens;

8° gevallen waarbij de bankrekening van een persoon gebruikt wordt om onrechtmatig fondsen van derden te ontvangen en/of door te sturen, met de bedoeling hiermee de identiteit van deze derden te verhullen.

9° gevallen van fraude met en vervalsing van niet-contante betaalmiddelen in de zin van het wetsontwerp tot omzetting van Richtlijn 2019/713 van het Europees Parlement en de Raad van 17 april 2019 betreffende de bestrijding van fraude met en vervalsing van niet-contante betaalmiddelen en ter vervanging van Kaderbesluit 2001/413/JBZ van de Raad.

De Koning kan de categorieën van incidenten zoals bedoeld in het eerste lid verder aanvullen.

§ 2. De door de betrokken instelling krachtens artikel 9, tweede lid, aangewezen bevoegde personen dienen steeds de afweging te maken of voldaan is aan één of meer van de in paragraaf 1 omschreven gevallen. Bij twijfel wordt over al dan niet registratie in het voordeel van de aan het incident gerelateerde persoon beslist.

De beslissing mag niet leiden tot de registratie van een persoon wanneer op basis van

démontré sur base de plusieurs éléments concordants qu'elle est victime de l'incident, et ce, conformément au but du système d'alerte visé à l'article 3, alinéa 2, 3°.

Cette décision est motivée et documentée par les personnes désignées par l'établissement concerné. La décision des établissements concernés d'enregistrer une personne est prise dans un délai raisonnable sur la base des critères objectifs suivants :

1° la gravité de l'incident ;

2° la question de savoir s'il est question de tentatives détectées ou ratées ou de préparations de commission d'un incident ;

3° si d'application, le montant sur lequel l'incident porte ;

4° le fait que la personne (morale) a déjà été enregistrée concernant un autre incident ;

5° la mesure dans laquelle l'incident a porté préjudice ou peut porter préjudice à l'établissement concerné ou à ses clients.

§ 3. Les établissements concernés ne laissent aucune conséquence découler du simple enregistrement d'une personne, qui entraînerait que la personne enregistrée serait automatiquement exclue du système financier. Par conséquent, l'accès au crédit et aux services de paiement continue à s'appliquer conformément aux dispositions du livre VII du Code de droit économique. Le système sert d'alerte de risque des actes visés dans la loi.

Les données mises à disposition par le système servent à soutenir l'évaluation et l'analyse des risques déjà existantes des établissements concernés.

Article 6. Description des données d'alerte

Les données suivantes des personnes qui manifestent des comportements donnant lieu à

meerdere overeenstemmende elementen wordt aangetoond dat hij het slachtoffer is van het incident, en dit overeenkomstig het doel van het waarschuwingssysteem bedoeld in artikel 3, tweede lid, 3°.

Deze besluitvorming wordt door de betrokken instelling aangewezen personen gemotiveerd en gedocumenteerd. De beslissing van de betrokken instellingen om een persoon te registreren gebeurt binnen een redelijke termijn op basis van volgende objectieve criteria:

1° de ernst van het incident;

2° of er sprake is van gedetecteerde of mislukte pogingen of voorbereidingen tot het plegen van een incident;

3° waar van toepassing, het bedrag waarop het incident betrekking heeft;

4° het feit of de (rechts)persoon reeds met betrekking tot een ander incident geregistreerd werd;

5° de mate waarin het incident schade heeft berokkend of kan berokkenen aan de betrokken instelling of haar klanten.

§ 3. De betrokken instellingen laten geen gevolgen voortvloeien uit de loutere registratie van een persoon waarbij de geregistreerde persoon automatisch van het financiële systeem uitgesloten zouden worden. Bijgevolg blijft de toegang tot krediet- en betalingsdiensten van toepassing overeenkomstig de bepalingen van boek VII van het Wetboek van economisch recht. Het systeem geldt als een risicowaarschuwing voor de in de wet bedoelde handelingen.

De door het systeem beschikbaar gestelde gegevens dienen ter ondersteuning van de reeds bestaande risico-inschatting en analyse van de betrokken instellingen.

Artikel 6. Beschrijving van de waarschuwingsgegevens

Van zij die de gedragingen stellen die leiden tot incidenten en van zij die aan deze gedragingen

des incidents et des personnes qui contribuent à ces comportements sont enregistrées dans le registre d'alerte :

1° les données d'identification de la personne physique ou morale :

a) le numéro de compte ;

b) les nom, prénoms, date de naissance et lieu de naissance de la personne physique ;

c) la dénomination sociale et le numéro d'entreprise de la personne morale ;

2° les données concernant l'incident :

a) le type d'incident sur la base de l'article 5, § 1^{er} ;

b) la description de la méthode de travail ;

3° les données concernant l'enregistrement :

a) le numéro de référence ;

b) la date de l'enregistrement ;

c) la dénomination sociale, le numéro d'entreprise et le code BIC (Bank Identifier Code) de l'établissement concerné qui procède à l'enregistrement ;

d) la notification ou non de l'enregistrement à la personne impliquée dans un incident conformément à l'article 12.

Le Roi peut compléter et/ou adapter les catégories et le type de données visées à l'alinéa 1^{er}, à l'exception des données à caractère personnel.

Article 7. Délai de conservation

Le délai de conservation des données d'alerte est de dix ans maximum à compter de la date d'enregistrement.

Section 4. Gestion du et accès au système et

meewerken, worden volgende gegevens in het waarschuwingsregister geregistreerd :

1° identificatiegegevens van de natuurlijke persoon of rechtspersoon:

a) rekeningnummer;

b) naam, voornamen, geboortedatum en geboorteplaats van de natuurlijke persoon ;

c) naam en ondernemingsnummer van de rechtspersoon;

2° gegevens betreffende het incident:

a) type incident op basis van artikel 5, § 1;

b) omschrijving van de werkwijze;

3° gegevens met betrekking tot de registratie:

a) referentienummer;

b) datum registratie;

c) naam, ondernemingsnummer en BIC (Bank Identifier Code) van de betrokken instelling die tot de registratie overgaat;

d) de, al dan niet, bekendmaking van de registratie aan de persoon betrokken in een incident overeenkomstig artikel 12.

De Koning kan de categorieën en type van gegevens zoals voorzien onder het eerste lid, met uitzondering van persoonsgegevens, verder aanvullen en/of aanpassen.

Artikel 7. Bewaartermijn

De bewaartermijn van de waarschuwingsgegevens bedraagt maximaal tien jaar vanaf de datum van registratie.

Afdeling 4. Beheer van en toegang tot het systeem en uitwisseling van

échange de données d'alerte

waarschuwingsgegevens

Article 8. Responsabilité à l'égard du système

Chaque établissement concerné est responsable à l'égard du système. En ce sens, les établissements concernés sont chacun également des responsables distincts et indépendants du traitement au sens du Règlement général sur la protection des données.

En tant que responsables du traitement, les établissements concernés prennent les mesures techniques et organisationnelles nécessaires pour démontrer que le présent traitement de données à caractère personnel se déroule conformément au Règlement général sur la protection des données.

Article 9. Accès et gestion

Les établissements concernés désignent les personnes compétentes dans le cadre de la gestion du système. Seules ces personnes qui, dans le cadre de leur fonction et de leurs missions, doivent collecter, traiter et mettre à jour les données enregistrées dans le registre d'alerte sont compétentes pour accéder au système.

Les personnes autres que les personnes et établissements concernés visés à l'alinéa 1^{er} n'ont pas accès au système.

Article 10. Échange d'informations

Les données d'alerte sont partagées de manière sécurisée et structurelle entre les établissements concernés. Les informations partagées concernent tant les nouvelles données que les données mises à jour et/ou la suppression de données enregistrées.

La manière de procéder et la technologie qui sera utilisée seront définies dans un Protocole

Artikel 8. Verantwoordelijkheid voor het systeem

Elke betrokken instelling is verantwoordelijk voor het systeem. In die zin zijn de betrokken instellingen ook elk afzonderlijke en onafhankelijke verwerkingsverantwoordelijken in de zin van de Algemene Verordening Gegevensbescherming.

Als verwerkingsverantwoordelijke nemen de betrokken instellingen de nodige technische en organisatorische maatregelen ten einde aan te tonen dat de voorliggende verwerking van persoonsgegevens in overeenstemming met de Algemene Verordening Gegevensbescherming verloopt.

Artikel 9. Toegang en beheer

De betrokken instellingen stellen de bevoegde personen aan in het kader van het beheer van het systeem. Alleen deze personen die in het kader van hun functie en opdrachten de gegevens opgenomen in het waarschuwingsregister moeten verzamelen, verwerken en bijwerken, zijn bevoegd om toegang te krijgen tot het systeem.

Andere dan de in het eerste lid bedoelde personen en betrokken instellingen hebben geen toegang tot het systeem.

Artikel 10. Uitwisseling van informatie

De waarschuwingsgegevens worden op een structurele manier tussen de betrokken instellingen op een beveiligde manier gedeeld. De gedeelde informatie betreft zowel nieuwe gegevens, bijgewerkte gegevens en/of de verwijdering van geregistreerde gegevens.

De manier waarop en de technologie die gebruikt zal worden zal in een Protocol

conclu entre les établissements concernés.

vastgelegd worden tussen de betrokken instellingen.

Si l'enregistrement des données dans le registre d'alerte compromet une enquête en cours, les établissements concernés sont dispensés de les enregistrer dans le registre d'alerte et de partager les informations avec un autre établissement concerné.

Indien het opnemen van de gegevens in het waarschuwingsregister een lopend onderzoek in het gedrang zou brengen, zijn de betrokken instellingen vrijgesteld om dit in het waarschuwingsregister op te nemen en de informatie te delen met een andere betrokken instelling.

Sur la base de l'échange de ces données d'alerte, les personnes compétentes des établissements concernés sont autorisées à prendre contact de manière bilatérale entre elles afin de fournir davantage d'informations sur l'incident en question qui a conduit à l'enregistrement dans le registre d'alerte aux mêmes conditions que celles prévues dans la présente loi.

Op basis van de uitwisseling van deze waarschuwingsgegevens zijn de bevoegde personen van de betrokken instellingen toegelaten om bilateraal contact te nemen met elkaar om meer informatie te verschaffen over het betrokken incident dat aanleiding heeft gegeven tot de registratie in het waarschuwingsregister onder dezelfde voorwaarden zoals voorzien in deze wet.

Section 5. Informations concernant le système d'alerte d'incidents et notification de l'enregistrement

Afdeling 5. Informatie over het Incidentenwaarschuwingssysteem en bekendmaking registratie

Article 11. Informations concernant le système

Artikel 11. Informatie over het systeem

Des informations transparentes sur l'existence et le fonctionnement du système sont mises à disposition des personnes concernées par tous les établissements concernés dans un langage et sous une forme compréhensibles et accessibles, par les canaux numériques ou par courrier.

Transparante informatie over het bestaan en de werking van het systeem worden door alle betrokken instellingen aan de betrokken personen ter beschikking gesteld in een begrijpelijke en toegankelijke taal en vorm, via digitale kanalen of duurzame drager.

Article 12. Communication concernant l'enregistrement

Artikel 12. Bekendmaking van de registratie

Il appartient à l'établissement concerné qui enregistre les données de la personne impliquée dans un incident dans le registre d'alerte d'incidents de porter cet enregistrement à la connaissance de la personne enregistrée.

Het behoort aan de betrokken instelling die de gegevens van de persoon betrokken in een incident in het waarschuwingsregister opneemt, om deze registratie aan de geregistreerde persoon bekend te maken.

Si l'incident donne lieu à une enquête de police et/ou à une instruction et que la communication à la personne enregistrée peut entraver l'enquête, la détection et la poursuite

Indien het incident aanleiding geeft tot een politie- en/of gerechtelijk onderzoek en de bekendmaking aan de geregistreerde persoon het onderzoek, de opsporing en de vervolging

d'infractions pénales et/ou l'exécution de peines et/ou peut compromettre la protection de la victime, la communication à la personne enregistrée n'interviendra, conformément à l'article 14, qu'après la clôture de l'enquête de police et/ou de l'instruction et sa prise de connaissance par l'établissement concerné.

van strafbare feiten en/of de tenuitvoerlegging van straffen kan verhinderen en/of de bescherming van het slachtoffer in het gevaar kan brengen, zal de bekendmaking aan de geregistreerde persoon, overeenkomstig artikel 14, pas plaatsvinden na het afsluiten van het politie- en/of gerechtelijk onderzoek en de kennisname hiervan door de betrokken instelling.

Section 6. Droits de la personne en rapport avec l'incident

Afdeling 6. Rechten van de aan het incident gerelateerde persoon

Article 13. Droit à la contradiction

Artikel 13. Recht op tegenspraak

§ 1^{er}. Toute personne dont les données ont été enregistrées dans le registre d'alerte a la possibilité de contester cet enregistrement auprès de l'établissement concerné qui y a procédé. À cet égard, la personne enregistrée peut apporter de nouveaux éléments susceptibles d'influencer la décision de procéder à l'enregistrement.

§ 1. Eenieder wiens gegevens in het waarschuwingsregister geregistreerd werden, krijgt de mogelijkheid om deze registratie, bij de betrokken instelling die de registratie uitvoerde, te betwisten. Hierbij kan de geregistreerde persoon nieuwe elementen aandragen die de beslissing tot registratie kunnen beïnvloeden.

§ 2. Ce droit peut être exercé dans les 30 jours calendrier de la communication de l'enregistrement à la personne enregistrée au sens de l'article 12.

§ 2. Dit recht kan worden uitgeoefend binnen de 30 kalenderdagen na mededeling van de registratie aan de geregistreerde persoon in de zin van artikel 12.

§ 3. Les établissements concernés fournissent un formulaire standard qui peut être utilisé par la personne enregistrée pour l'exercice du droit défini au paragraphe 2. Ce formulaire est rendu accessible publiquement.

§ 3. De betrokken instellingen voorzien in een standaardformulier dat door de geregistreerde persoon gebruikt kan worden voor het uitoefenen van het in paragraaf 2 bepaalde recht. Dit formulier wordt publiek toegankelijk gemaakt.

§ 4. Dans les 30 jours de la réception de la contestation, l'établissement concerné prend une décision quant à la prise en considération des objections formulées. La personne enregistrée est informée par écrit de cette décision.

§ 4. Binnen de 30 dagen na ontvangst van de tegenspraak neemt de betrokken instelling een beslissing of er met de gemaakte opmerkingen rekening kan worden gehouden. De geregistreerde persoon wordt schriftelijk geïnformeerd over deze beslissing.

Une contestation est fondée s'il ressort que les conditions d'enregistrement prévues à l'article 5 n'ont pas été remplies, ou si l'enregistrement n'a pas été suffisamment motivé.

Een tegenspraak is gegrond indien hieruit blijkt dat de voorwaarden voor registratie zoals bepaald in artikel 5 niet vervuld zijn, of indien de registratie onvoldoende gemotiveerd werd.

§ 5. Si une contestation est jugée fondée, les

§ 5. Indien een tegenspraak gegrond bevonden

données concernées sont supprimées sans délai du système et tous les établissements concernés en sont informés.

wordt, worden de betrokken gegevens onverwijld verwijderd uit het systeem en worden alle betrokken instellingen hierover geïnformeerd.

Article 14. Droits fondés sur le Règlement général sur la protection des données

Artikel 14. Rechten op basis van de Algemene Verordening Gegevensbescherming

En vertu du Chapitre III du Règlement général sur la protection des données, les personnes physiques en rapport avec l'incident disposent, en tant que personnes concernées, de différents droits énumérés aux articles 12 à 22 du règlement précité.

Krachtens Hoofdstuk III van de Algemene Verordening Gegevensbescherming beschikken de aan het incident gerelateerde natuurlijke personen, als betrokkenen, over verschillende rechten zoals opgesomd in de artikelen 12 tot 22 van voornoemde verordening.

Conformément à l'article 23.1, d) et i), du Règlement général sur la protection des données, les articles 12 à 22 de ce règlement ne sont toutefois pas applicables au traitement de données à caractère personnel par l'établissement concerné si son application peut entraver une enquête de police et/ou une instruction ou la détection et la poursuite d'infractions pénales et/ou l'exécution de peines et/ou peut compromettre la protection de la victime. Cette dispense s'applique à toutes les catégories de données à caractère personnel pour autant que ce soit conforme à la finalité du présent paragraphe.

Overeenkomstig artikel 23.1, d) en i) van de Algemene Verordening Gegevensbescherming zijn de artikelen 12 tot 22 van deze verordening evenwel niet van toepassing voor de verwerking van persoonsgegevens door de betrokken instelling indien de toepassing ervan een politie en/of gerechtelijk onderzoek of de opsporing en de vervolging van strafbare feiten en/of de tenuitvoerlegging van straffen kan verhinderen en/of de bescherming van het slachtoffer in het gevaar kan brengen. Deze vrijstelling geldt voor alle categorieën van persoonsgegevens en voor zover het in overeenstemming is met het doeleinde van huidige paragraaf.

Le délégué à la protection des données désigné en vertu du Chapitre IV, Section 4, du Règlement général sur la protection des données auprès de l'établissement concerné qui a procédé à l'enquête et/ou à l'enregistrement et/ou les personnes chargées de telles tâches au sein de l'établissement concerné servent de premier point de contact pour l'exercice des droits de la personne enregistrée sur la base de ce règlement.

De krachtens Hoofdstuk IV, Afdeling 4 van de Algemene Verordening Gegevensbescherming bij de betrokken instelling die tot onderzoek en/of registratie overging, aangestelde functionaris voor gegevensbescherming en/of de personen belast met dergelijke taken binnen de betrokken instelling, geldt als eerste aanspreekpunt voor de uitoefening van de rechten van de geregistreerde persoon op basis van deze verordening.

L'établissement concerné informe la personne concernée de ses droits définis aux articles 12 à 22 du Règlement général sur la protection des données ainsi que des motifs de refus ou de limitation. Les informations relatives au refus ou à la limitation doivent être omises si leur communication devait nuire aux objectifs de l'alinéa 2.

De betrokken instelling informeert de betrokkene over zijn rechten bepaald in de artikelen 12 tot 22 van de Algemene Verordening Gegevensbescherming alsook over de redenen van weigering of beperking. De informatie over de weigering of beperking moet achterwege worden gelaten wanneer de verstrekking ervan een van de doelstellingen van het tweede lid zou ondermijnen.

Section 7. Litiges

Afdeling 7. Geschillen

Article 15. Litiges

Outre les droits et procédures de la défense prévus aux articles 13 et 14 et après application préalable de ces droits et procédures, les personnes physiques enregistrées peuvent déposer une plainte auprès du service de médiation en conflits financiers OMBUDSFIN.

Artikel 15. Geschillen

Naast de verdedigingsrechten en -procedures zoals voorzien onder artikel 13 en artikel 14 en na voorafgaandelijke toepassing van deze rechten en procedures, kunnen de geregistreerde natuurlijke personen een klacht indienen bij de Ombudsdienst in financiële geschillen OMBUDSFIN.

Section 8. Entrée en vigueur

Afdeling 8. Inwerkingtreding

Article 16. Entrée en vigueur

La présente loi entre en vigueur le premier jour du douzième mois qui suit celui de sa publication au Moniteur belge.

Artikel 16. Inwerkingtreding

Deze wet treedt in werking op de eerste dag van de twaalfde maand na die waarin ze is bekendgemaakt in het Belgisch Staatsblad.

Le Ministre des Finances,

De Minister van Financiën,

VINCENT VAN PETEGHEM

Le Ministre de la Justice,

De Minister van Justitie,

A stylized, handwritten signature in blue ink. It features a large, circular loop on the left side, followed by a horizontal line that extends to the right and then curves upwards and to the right, ending in a sharp, upward-pointing stroke.

VINCENT VAN QUICKENBORNE

ROYAUME DE BELGIQUE

KONINKRIJK BELGIE

SERVICE PUBLIC FÉDÉRAL JUSTICE ET FINANCES

FEDERALE OVERHEIDSDIENST JUSTITIE EN
FINANCIEN

**Avant-projet de loi portant création d'un
système d'alerte d'incident dans le secteur
financier**

**Voorontwerp van wet houdende de oprichting
van een incidentenwaarschuwingssysteem
binnen de financiële sector**

EXPOSÉ DES MOTIFS

MEMORIE VAN TOELICHTING

MESDAMES, MESSIEURS,

DAMES EN HEREN,

CONSIDÉRATIONS GÉNÉRALES

ALGEMENE BESCHOUWINGEN

Le présent avant-projet de loi a pour objet de prévoir un cadre légal visant à garantir l'intégrité du secteur financier dans le cadre de la lutte contre l'usage abusif de services financiers et les éventuels dommages qui peuvent en découler tant pour les établissements financiers que pour les citoyens et les pouvoirs publics, et ce, au moyen de la création d'un système qui permet aux acteurs du secteur financier de s'alerter mutuellement et d'échanger des informations et des données de manière sécurisée afin de prévenir les fraudes.

Dit voorontwerp van wet heeft tot doel een wettelijk kader te voorzien voor het waarborgen van de integriteit van de financiële sector in het kader van de strijd tegen het oneigenlijk gebruik van financiële diensten en de mogelijke schade die daaruit voort kan vloeien voor zowel de financiële instellingen, de burgers als de overheid, en dit, middels de oprichting van een systeem dat de actoren binnen de financiële sector toelaat elkaar onderling te waarschuwen en, op een beveiligde manier, informatie en gegevens met elkaar uit te wisselen om fraude te voorkomen.

I. Contexte

I. Achtergrond

Les acteurs financiers jouent un rôle essentiel dans la lutte contre l'usage abusif de services financiers. Sur la base de diverses lois comme la loi relative au statut et au contrôle des établissements de crédit¹ et la loi relative au statut des établissements de paiement², les acteurs financiers, entre autres, sont tenus de prendre des mesures de gestion des risques appropriées contre des risques et incidents

Financiële actoren spelen een essentiële rol in de strijd tegen het oneigenlijk gebruik van financiële diensten. Op basis van verschillende wetgeving, zoals de wet op het statuut van en het toezicht op de kredietinstellingen³ en de wet op het statuut van de betalingsinstellingen⁴, zijn bijvoorbeeld financiële actoren gehouden passende risicobeheersmaatregelen te nemen tegen bijzondere risico's en incidenten om de

¹ Loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit, *M.B.* 7 mai 2014.

² Loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement, et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement, *M.B.* 26 mars 2018.

³ Wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen, *B.S.* 7 mei 2014.

⁴ Wet van 11 maart 2018 betreffende het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld, en de toegang tot betalingssystemen, *B.S.* 26 maart 2018.

particuliers afin d'assurer la sécurité et l'intégrité du secteur financier. Les établissements de crédit ont ainsi l'obligation légale de conserver des données bancaires et d'établir des procédures internes permettant de détecter plus facilement des transactions suspectes.

Les acteurs financiers sont toutefois de plus en plus souvent confrontés à des risques et des fraudes (ou tentatives de fraude) plus complexes. Les auteurs n'ont plus uniquement recours aux méthodes classiques comme la fraude à l'identité, mais se servent également de divers mécanismes technologiques nouveaux comme l'écroulement (skimming), l'hameçonnage (phishing), l'hameçonnage par SMS (smishing), l'espionnage par-dessus l'épaule (shoulder surfing)... En outre, en raison de la numérisation de la société, la fraude est commise à une échelle toujours plus grande pouvant éventuellement toucher plusieurs établissements à la fois. Ainsi, les acteurs financiers constatent régulièrement que certaines typologies de fraude se répètent dans différents établissements. De plus, de tels cas ne se limitent pas aux services de paiement, mais affectent également d'autres services comme les crédits.

Afin d'éviter que ces nouveaux risques ne constituent un danger pour la continuité et l'intégrité du secteur financier et de préserver les intérêts des clients, les acteurs financiers doivent adapter leurs mesures de maîtrise des risques aux circonstances changeantes. Les possibilités légales actuelles d'échange de données par des acteurs financiers dans le cadre de la lutte contre la fraude laissent toutefois peu de marge pour répondre à ces circonstances changeantes.

L'Europe attend elle aussi depuis longtemps, notamment des établissements de crédit, qu'ils jouent un rôle actif en matière de lutte contre la fraude. En 1998 déjà, une communication de la Commission européenne relative à la prévention de la fraude en matière de paiements réservait

véloce et intégrité van de financiële sector te verzekeren. Zo hebben kredietinstellingen de wettelijke verplichting om bankgegevens te bewaren en interne procedures op te zetten om verdachte transacties makkelijker te detecteren.

Financiële actoren worden echter steeds vaker geconfronteerd met complexere risico's en (pogingen tot) fraude. Daders maken niet langer enkel gebruik van klassieke methodes zoals identiteitsfraude, maar benutten diverse nieuwe technologische mechanismen, waaronder skimming, phishing, smishing, shoulder surfing, De digitalisering van de maatschappij zorgt er bovendien voor dat fraude op een steeds grotere schaal wordt gepleegd, waarbij mogelijk meerdere instellingen tegelijk betrokken raken. Zo stellen financiële actoren regelmatig vast dat bepaalde fraudetypologieën zich herhalen bij verschillende instellingen. Ook blijven dergelijke gevallen niet enkel beperkt tot betalingsdiensten, maar treft het ook andere diensten zoals kredieten.

Om te voorkomen dat deze nieuwe risico's een gevaar vormen voor de continuïteit en de integriteit van de financiële sector, alsmede ter vrijwaring van de belangen van de cliënten, dienen financiële actoren hun risico-beheersende maatregelen structureel aan te passen aan de veranderende omstandigheden. De huidige wettelijke mogelijkheden voor het uitwisselen van gegevens door financiële actoren in het kader van fraudebestrijding laten echter weinig ruimte om te beantwoorden aan deze veranderende omstandigheden.

Ook vanuit Europa wordt al geruime tijd een actieve rol verwacht van onder meer de kredietinstellingen met betrekking tot fraudebestrijding. Al in 1998 vaardigde de Europese Commissie een mededeling uit betreffende fraudepreventie inzake betalingen waarin ook een rol weggelegd werd voor

également un rôle aux établissements de crédit.⁵ kredietinstellingen.⁶

Cette communication a été suivie, en 2001, d'un plan d'action dans lequel la Commission européenne appelait le secteur des paiements à échanger des informations en vue d'« *une détection et d'une notification plus rapides des tentatives de fraude* ».⁷

De même, le plan d'action de 2004 pour la prévention de la fraude réitérait l'appel à l'échange d'informations.⁹

Dans une consultation de la Commission européenne, l'importance d'une lutte effective contre la fraude a été soulignée une nouvelle fois.¹¹ Le document de consultation y afférent parle de la nécessité d'un échange de données effectif provenant du secteur privé.¹²

Il y a une volonté manifeste du législateur européen de permettre l'échange d'informations entre acteurs du secteur

Deze mededeling werd opgevolgd door een actieplan uit 2001, waarin de Europese Commissie de betalingssector oproept om informatie uit te wisselen om de “*spoedige opsporing en kennisgeving van fraudepogingen mogelijk te maken*”.⁸

Ook in het actieplan betreffende fraudebestrijding uit 2004 werd de oproep tot het uitwisselen van informatie herhaald.¹⁰

In een consultatie door de Europese Commissie werd andermaal het belang van effectieve fraudebestrijding onderstreept.¹³ Het bijhorende consultatiedocument spreekt hierbij over de nood aan effectieve gegevensdeling vanuit de private sector.¹⁴

Er is een duidelijke wil van de Europese wetgever om de uitwisseling van informatie tussen actoren in de financiële sector mogelijk te maken

⁵ Communication de la Commission au Parlement européen, au Conseil, à la Banque centrale européenne et au Comité économique et social – Un cadre d'action pour lutter contre la fraude et la contrefaçon des moyens de paiement autres que les espèces, COM(1998)395.

⁶ Mededeling van de Commissie aan het Europees Parlement, de Raad, de Europese Centrale Bank en het Economisch en Sociaal Comité – Een actiekader voor de bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten, COM(1998)395.

⁷ Communication de la Commission au Conseil, au Parlement européen, à la Banque centrale européenne, au Comité économique et social et à Europol - Prévention de la fraude et de la contrefaçon des moyens de paiement autres que les espèces, COM(2001)11, 5-6.

⁸ Mededeling van de Commissie aan de Raad, het Europees Parlement, de Europese Centrale Bank, het Economisch en Sociaal Comité en Europol - Preventie van fraude en vervalsing van girale betaalmiddelen, COM(2001)11, 5-6.

⁹ Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social européen, à la Banque centrale européenne et à Europol - Un nouveau Plan d'action de l'UE (2004-2007) pour la prévention de la fraude sur les moyens de paiement autres que les espèces, COM(2004)679, 6-7.

¹⁰ Mededeling van de Commissie aan de Raad, het Europees Parlement, het Europees Economisch en Sociaal Comité, de Europese Centrale Bank en Europol - Een nieuw Actieplan van de Europese Unie (2004-2007) voor de preventie van fraude met girale betaalmiddelen, COM(2004)679, 6-7.

¹¹ https://home-affairs.ec.europa.eu/system/files/2020-09/20170406_publication_fr.pdf

¹² Commission européenne (2016) “Combatting Fraud and Counterfeiting of Non-Cash Means of Payment”, 2016/HOME/077, 4-5 et 7-8.

¹³ https://ec.europa.eu/home-affairs/content/consultation-initiative-combatting-fraud-counterfeiting-non-cash-payment_en.

¹⁴ Europese Commissie (2016) “Combatting Fraud and Counterfeiting of Non-Cash Means of Payment”, 2016/HOME/077, 4-5 en 7-8.

financier dans le cadre de formes bien définies de lutte contre la fraude. Cette volonté est, par ailleurs, également soulignée dans deux nouveaux textes. D'une part, dans un règlement concernant la résilience opérationnelle numérique du secteur financier.¹⁵ L'article 40 de ce règlement permet, en effet, aux entités financières d'« *échanger entre elles des informations et des renseignements sur les cybermenaces, notamment des indicateurs de compromis, des tactiques, des techniques et des procédures, des alertes cybersécurité et des outils de configuration, dans la mesure où ce partage d'informations et de renseignements vise à améliorer la résilience opérationnelle numérique des entités financières, notamment en les sensibilisant aux cybermenaces, en limitant ou en bloquant la capacité de propagation des cybermenaces, et en soutenant l'éventail de capacités défensives, de techniques de détection des menaces et de stratégies d'atténuation des entités financières, ou leurs phases de réponse et de rétablissement* », et ce, dans le respect notamment de la réglementation en matière de protection des données à caractère personnel.¹⁶ D'autre part, cette volonté est également accentuée dans la directive concernant un niveau élevé commun de cybersécurité (dite la Directive SRI 2)¹⁷, dont l'article 29 impose aux États membres d'élaborer un cadre réglementaire pour un échange de données similaire à celui figurant dans le règlement précité. Ce souhait a d'ailleurs été exprimé

in het kader van welbepaalde vormen van fraudebestrijding. Deze wil wordt nog verder onderstreept in twee nieuwe teksten. Enerzijds in een verordening betreffende digitale operationele veerkracht voor de financiële sector.¹⁸ Artikel 45 van deze verordening laat financiële entiteiten immers toe om “*onderling informatie en inlichtingen over cyberdreiging uit [te] wisselen, met inbegrip van indicators of compromise, tactieken, technieken en procedures, cyberbeveiligingswaarschuwingen en configuratie-instrumenten*”, voor zover dit “*tot doel heeft de digitale operationele veerkracht van financiële entiteiten te versterken, met name via bewustmaking met betrekking tot cyberdreigingen, beperking of belemmering van de mogelijkheid tot verdere verspreiding van cyberdreigingen, ondersteuning van het gamma aan defensieve capaciteiten van financiële entiteiten, dreigingsdetectietechnieken, risicobeperkende strategieën of respons- en herstelfasen*” en gebeurt met inachtneming van onder meer de regelgeving inzake de bescherming van persoonsgegevens.¹⁹ Anderzijds wordt deze wil ook benadrukt in de richtlijn inzake een hoog gemeenschappelijk niveau van cybersecurity (de zogenaamde NIS2-Richtlijn)²⁰, waarvan artikel 29 de Lidstaten oplegt om een regelgevend kader uit te werken voor een gelijkaardige gegevensuitwisseling als deze uit voornoemde verordening. Deze wil werd trouwens recent geuit middels de resolutie betreffende het bestrijden van cyberfraude via geldezels zoals

¹⁵ Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements n° 1060/2009, (EU), n° 648/2012, (EU) n° 600/2014, (EU), n° 909/2014 et (EU) 2016/1011

¹⁶ *Id.*

¹⁷ Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la Directive (UE) 2018/1972 et abrogeant la Directive (UE) 2016/1148 (directive SRI 2).

¹⁸ Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG), nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 et (EU) 2016/1011.

¹⁹ *Id.*

²⁰ Richtlijn (EU) 2022/2555 van het Europees Parlement en Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU), nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-Richtlijn).

récemment par le biais d'une résolution relative à la lutte contre la cyberfraude utilisant des mules bancaires, telle qu'adoptée le 17 février 2022 à la Chambre des représentants et dans laquelle il est plaidé en faveur de l'élaboration d'un cadre légal qui permette aux établissements financiers d'échanger des informations entre eux.

Il est toutefois également reconnu que les informations qui devraient être échangées pourraient concerner la vie privée de la personne enregistrée. Par conséquent, il convient de respecter un équilibre « *entre les intérêts de la prévention de la fraude et le respect des droits fondamentaux des personnes* ». ²¹

Cette considération figure également dans un document consultatif de 2003 concernant un cadre juridique pour les paiements dans le marché intérieur. Ce document souligne d'une part l'utilité de signaux de signalisation sectoriels, mais d'autre part également la possibilité de conflits entre un tel échange d'informations et le droit à la protection des données. ²³ Ainsi, la Commission européenne renvoie dans ce document à la disposition dérogatoire de l'article 13, point d), de la directive 95/46/CE, qui permet de déroger aux principes de la protection des données pour assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales.

Cette disposition de la directive relative à la protection des données n'a toutefois pas été transposée de la même manière dans tous les États membres, ce qui a donné lieu à une fragmentation du droit de la protection des données qui entrave l'échange d'informations en lien avec la fraude. La solution proposée

aangenen door de Kamer van volksvertegenwoordiger op 17 februari 2022 en waarin er gepleit wordt voor het uitwerken van een wettelijk kader dat de financiële instellingen zou toelaten informatie met elkaar uit te wisselen.

Er wordt echter ook erkend dat de informatie die uitgewisseld zou moeten worden mogelijk de privacy van de geregistreerde persoon aanbelangt. Bijgevolg moet een afweging gemaakt worden "*tussen de belangen van de fraudepreventie en de inachtneming van de individuele grondrechten*". ²²

Deze overweging werd ook aangehaald in een raadplegingsdocument betreffende een rechtskader voor betalingen in de interne markt uit 2003, waarbij enerzijds het nut van sectorale signaalsystemen benadrukt werd, maar anderzijds ook de mogelijkheid van conflicten tussen dergelijke informatie-uitwisseling en het recht op gegevensbescherming onderstreept werd. ²⁴ Zo verwijst de Europese Commissie in dat document naar de uitzonderingsbepaling van artikel 13(d) van Richtlijn 95/46/EG, die een afwijking op de principes van gegevensbescherming toestaat met het oog op de preventie, het onderzoek, de opsporing en de vervolging van strafbare feiten.

Die bepaling uit de richtlijn gegevensbescherming werd echter niet in alle Lidstaten gelijkwaardig omgezet, wat geleid heeft tot een versnippering in het gegevensbeschermingsrecht die de uitwisseling van fraude-gerelateerde informatie bemoeilijkt. De oplossing die voorgesteld werd, zou bestaan

²¹ Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social européen, à la Banque centrale européenne et à Europol - Un nouveau Plan d'action de l'UE (2004-2007) pour la prévention de la fraude sur les moyens de paiement autres que les espèces, COM(2004)679, 6-7.

²² Mededeling van de Commissie aan de Raad, het Europees Parlement, het Europees Economisch en Sociaal Comité, de Europese Centrale Bank en Europol - Een nieuw Actieplan van de Europese Unie (2004-2007) voor de preventie van fraude met girale betaalmiddelen, COM(2004)679, 6-7.

²³ Communication de la Commission au Conseil et au Parlement européen concernant un nouveau cadre juridique pour les paiements dans le marché intérieur (Document de consultation), COM(2003)718, 66-69.

²⁴ Mededeling van de Commissie aan de Raad en aan het Europees Parlement betreffende een nieuw rechtskader voor betalingen in de interne markt (raadplegingsdocument), COM(2003)718, 66-69.

consisterait en l'introduction d'une disposition dans le nouveau cadre juridique relatif aux paiements qui rendrait possible l'échange d'informations entre les acteurs dans le cadre de la lutte contre la fraude. Une telle disposition a été proposée pour la première fois dans la proposition de directive concernant les services de paiement dans le marché intérieur.²⁵

Cette disposition devrait finalement devenir l'article 79 de la directive concernant les services de paiement (2007/64/CE) et prévoit que les *« États membres autorisent le traitement des données à caractère personnel par les systèmes de paiement et les prestataires de services de paiement lorsque cela est nécessaire pour garantir la prévention, la recherche et la détection des fraudes en matière de paiements. Le traitement de ces données à caractère personnel est effectué conformément aux dispositions de la directive 95/46/CE. »* Cet article doit être lu conjointement avec le considérant 49, qui prévoit ce qui suit :

« Pour contribuer à une prévention efficace de la fraude et combattre la fraude en matière de paiements dans toute la Communauté, il y a lieu de prévoir un échange efficace de données entre les prestataires de services de paiement, qui devraient être autorisés à collecter, à traiter et à échanger des données à caractère personnel sur les personnes impliquées dans une fraude en matière de paiement. Toutes ces activités devraient être menées conformément à la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. »

La deuxième directive concernant les services de paiement (2015/2366/CE) réitère ce point à l'article 94 : *« Les États membres autorisent le traitement des données à caractère personnel par les systèmes de paiement et les prestataires*

uit het invoeren van een bepaling in het nieuwe rechtskader voor betalingen die informatie-uitwisseling tussen actoren in het kader van fraudebestrijding mogelijk zou maken. Dergelijke bepaling werd eerst voorgesteld in het voorstel voor een richtlijn betreffende betalingsdiensten in de interne markt.²⁶

Deze bepaling zou uiteindelijk artikel 79 van de richtlijn betalingsdiensten (2007/64/EG) worden, en stelt dat *“lidstaten staan toe dat betalingssystemen en betalingsdienstaanbieders persoonsgegevens verwerken wanneer zulks noodzakelijk is voor de voorkoming van, het onderzoek naar en de opsporing van betalingsfraude. De verwerking van dergelijke persoonsgegevens geschiedt in overeenstemming met Richtlijn 95/46/EG.”* Dit artikel moet samen met overweging 49 gelezen worden, welke bepaalt:

“Teneinde overal in de Gemeenschap effectieve fraudepreventie te bevorderen en betalingsfraude tegen te gaan, dient te worden voorzien in een efficiënte gegevensuitwisseling tussen betalingsdienstaanbieders, die ertoe moeten worden gemachtigd om persoonsgegevens over bij betalingsfraude betrokken personen te verzamelen, te verwerken en uit te wisselen. Al deze werkzaamheden dienen te worden verricht met inachtneming van Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.”

De tweede richtlijn betalingsdiensten, richtlijn 2015/2366/EU, herhaalt dit punt in artikel 94: *“De lidstaten staan toe dat betalingssystemen en betalingsdienstaanbieders persoonsgegevens verwerken wanneer zulks noodzakelijk is voor de*

²⁵ Proposition de directive du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur et modifiant les directives 97/7/CE, 2000/12/CE et 2002/65/CE, COM(2005)603, 53.

²⁶ Voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende betalingsdiensten in de interne markt en tot wijziging van de Richtlijnen 97/7/EG, 2002/12/EG en 2002/65/EG, COM(2005)603, 53.

de services de paiement lorsque cela est nécessaire pour garantir la prévention, la recherche et la détection des fraudes en matière de paiements. La communication aux personnes d'informations sur le traitement des données à caractère personnel et le traitement de ces données à caractère personnel ainsi que tout autre traitement de données à caractère personnel aux fins de la présente directive sont effectués conformément à la directive 95/46/CE et aux règles nationales transposant ladite directive, ainsi qu'au règlement (CE) no 45/2001. »²⁷ Cette disposition a été transposée en droit belge par le biais de l'article VII.63 du Code de droit économique.

Il convient en outre de renvoyer à l'article 105 de la directive 2015/2366/UE, dont il découle que les principes évoqués ci-avant en ce qui concerne le traitement de données à caractère personnel dans le cadre de la lutte contre la fraude en matière de paiements relèvent d'un régime d'harmonisation maximale. D'une part, il peut en être déduit que les États membres ont l'obligation de droit positif de permettre une telle lutte contre la fraude. D'autre part, les traitements dans le cadre d'une telle lutte contre la fraude en matière de paiements ne peuvent aller au-delà de l'objectif prescrit par les directives.

Les travaux du groupe de travail Article 29 avaient eux aussi déjà fait apparaître précédemment la possibilité de traiter - y compris d'échanger - des données à caractère personnel dans le cadre de la lutte contre la fraude. Ainsi, il est renvoyé dans « *Guidelines for Terminated Merchant Databases* » à la possibilité d'adopter une obligation légale comme fondement du traitement de données à caractère personnel dans le cadre de la

voorkoming van, het onderzoek naar en de opsporing van betalingsfraude. De verstrekking van informatie aan natuurlijke personen over de verwerking van persoonsgegevens en de verwerking van dergelijke gegevens en enige andere verwerking van persoonsgegevens voor de bij de onderhavige richtlijn beoogde doeleinden geschiedt overeenkomstig Richtlijn 95/46/EG, de nationale regelgeving tot omzetting van Richtlijn 95/46/EG en Verordening (EG) nr. 45/2001.»²⁸ Deze bepaling werd naar Belgisch recht omgezet door middel van artikel VII.63 van het Wetboek van Economisch Recht.

Daarnaast moet ook gewezen worden op artikel 105 van Richtlijn 2015/2366/EU, waaruit volgt dat de hierboven aangehaalde principes betreffende de verwerking van persoonsgegevens in het kader van fraudebestrijding inzake betalingen onder een regime van maximale harmonisatie vallen. Enerzijds kan hieruit worden afgeleid dat de Lidstaten de positiefrechtelijke verplichting hebben dergelijke fraudebestrijding mogelijk te maken. Anderzijds mogen de verwerkingen in het kader van dergelijke fraudebestrijding inzake betalingen niet ruimer gaan dan het doel voorgeschreven door de richtlijnen.

Ook de werkzaamheden van de Artikel 29 Werkgroep gaven al eerder blijk van de mogelijkheid tot het verwerken – inclusief de uitwisseling – van persoonsgegevens in het kader van fraudebestrijding. Zo wordt in de “*Guidelines for Terminated Merchant Databases*” verwezen naar de mogelijkheid tot het aannemen van een wettelijke verplichting als grondslag tot het verwerken van persoonsgegevens in het kader van

²⁷ Directive (UE) 2015/2366 du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) no 1093/2010, et abrogeant la directive 2007/64/CE, JO L 337/35.

²⁸ Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad betreffende betalingsdiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG, Pb. L 337/35.

prévention de la fraude.²⁹ En outre, dans une opinion concernant le traitement de données à caractère personnel dans le cadre de l'intérêt légitime du responsable du traitement, il est également renvoyé à la possibilité de traiter et d'échanger des données à caractère personnel dans le cadre de la lutte contre la fraude, pour autant que les mesures nécessaires à la protection des droits de la personne enregistrée soient prises.³⁰ Ici aussi, il est fait référence à la possibilité de prévoir un cadre légal qui prescrit un tel traitement.

Aujourd'hui, la conviction que des données à caractère personnel peuvent être traitées dans le cadre de la lutte contre la fraude fait également partie du droit de la protection des données même. Le considérant 47 du Règlement général sur la protection des données renvoie expressément à la possibilité, sur la base d'un intérêt légitime du responsable du traitement, de traiter des données à caractère personnel dans le cadre de la prévention de la fraude.³³ En outre, les États membres conservent le droit d'adopter une disposition légale qui prescrit un traitement déterminé – et ses modalités (considérant 45).

fraudepreventie.³¹ Bovendien wordt ook in een opinie omtrent de verwerking van persoonsgegevens in kader van het gerechtvaardigd belang van de verwerkingsverantwoordelijke verwezen naar de mogelijkheid tot het verwerken en uitwisselen van persoonsgegevens in het kader van fraudebestrijding, mits de nodige maatregelen ter bescherming van de rechten van de geregistreeerde persoon genomen worden.³² Ook hier wordt verwezen naar de mogelijkheid tot het voorzien van een wettelijk kader dat dergelijke verwerking voorschrijft.

De overtuiging dat persoonsgegevens verwerkt kunnen worden in het kader van fraudebestrijding is nu ook deel van het gegevensbeschermingsrecht zelf. Overweging 47 van de Algemene Verordening Gegevensbescherming verwijst expliciet naar de mogelijkheid om op grond van een gerechtvaardigd belang van de verwerkingsverantwoordelijke om persoonsgegevens te verwerken in het kader van fraudepreventie.³⁴ Bovendien behouden de Lidstaten het recht om wetgeving aan te nemen die een bepaalde verwerking – en de modaliteiten daartoe – voorschrijft (overweging 45).

²⁹ Groupe de travail Article 29 (2005), « Guidelines for Terminated Merchant Databases », https://ec.europa.eu/justice/article-29/documentation/other-document/files/2005/2005-01-11-fraudprevention_en.pdf, 3.

³⁰ Groupe de travail Article 29 (2014), « Opinion 06/2014 on the notion of legitimate interests of the data controller

under Article 7 of Directive 95/46/EC », WP217, 61-62.

³¹ Artikel 29 Werkgroep (2005) "Guidelines for Terminated Merchant Databases", https://ec.europa.eu/justice/article-29/documentation/other-document/files/2005/2005-01-11-fraudprevention_en.pdf, 3.

³² Artikel 29 Werkgroep (2014) "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC", WP217, 61-62.

³³ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données), *J.O.U.E.*, L 119, 4 mai 2016, 1-88.

³⁴ Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), *Pb.* L 119 van 4 mei 2016, 1-88.

II. Mise en œuvre de l'échange de données dans le cadre de la détection de fraude

Plusieurs États membres ont déjà répondu à l'appel de la Commission européenne en autorisant le traitement et le partage de données par des acteurs du secteur financier dans le cadre de la détection de fraude. Ainsi, il existe au Royaume-Uni le service Cifas, qui autorise les organisations participantes – principalement des établissements de crédit – à se notifier les uns aux autres des données relatives à des demandes potentiellement frauduleuses de produits ou de services ainsi que l'usage frauduleux de comptes et de services.³⁵ Aux Pays-Bas, il existe depuis 1997 déjà un « Incidentenwaarschuwingssysteem Financiële Instellingen » (système d'alerte d'incident institutions financières), dans le cadre duquel les établissements de crédit peuvent enregistrer et se notifier les uns aux autres des données de personnes (morales) qui ont fraudé ou qui constituent un risque d'une autre manière.³⁶

En Belgique, aucune initiative analogue n'a encore été prise jusqu'à présent. Par contre, des voix s'élèvent de plus en plus parmi les acteurs financiers pour demander le développement d'un système d'alerte d'incident. Un tel système d'alerte d'incident permettrait l'échange entre les acteurs financiers d'informations sur des incidents en lien avec la fraude et déterminés légalement. Une étroite collaboration et un partage de données entre les acteurs financiers favorisent la possibilité de détecter des incidents plus rapidement et plus efficacement grâce au fait que ces acteurs peuvent s'alerter les uns les autres. On peut de cette manière empêcher ou du moins réduire le risque d'autres transactions

II. Implementatie van gegevensuitwisseling in het kader van fraudedetectie

Verschillende Lidstaten hebben reeds de oproep van de Europese Commissie beantwoord door het verwerken en delen van gegevens door actoren in de financiële sector toe te staan in het kader van fraudedetectie. Zo bestaat in het Verenigd Koninkrijk de dienst Cifas, die deelnemende organisaties – hoofdzakelijk kredietinstellingen – toestaat gegevens met betrekking tot mogelijk frauduleuze aanvragen voor producten of diensten, alsook het frauduleus gebruik van rekeningen en diensten aan elkaar te melden.³⁷ In Nederland bestaat reeds sinds 1997 een Incidentenwaarschuwingssysteem Financiële Instellingen, waarbij kredietinstellingen gegevens van (rechts)personen die hebben gefraudeerd of op een andere manier een risico vormen kunnen registreren en aan elkaar melden.³⁸

In België is tot op heden nog geen gelijkaardig initiatief genomen. Er rijst bij financiële actoren wel een toenemende vraag naar de ontwikkeling van een systeem voor incidentenwaarschuwingen. Dergelijk incidentenwaarschuwingssysteem zou de uitwisseling van informatie over wettelijk bepaalde fraude-gerelateerde incidenten tussen financiële actoren mogelijk maken. Een nauwe samenwerking en gegevensdeling tussen financiële actoren faciliteert de mogelijkheid om incidenten sneller en efficiënter te detecteren doordat zij elkaar kunnen waarschuwen. Op deze manier kan men het risico op verdere frauduleuze transacties en daarmee gepaard

³⁵ <https://www.cifas.org.uk>.

³⁶ À cette fin, un protocole a été adopté au sein du secteur financier : <https://www.nvb.nl/publicaties/protocollen-regelingen-richtlijnen/protocol-incidenten-waarschuwingssysteem-financi%C3%ABle-instellingen>.

³⁷ <https://www.cifas.org.uk>.

³⁸ Hiertoe werd een protocol aangenomen binnen de financiële sector: <https://www.nvb.nl/publicaties/protocollen-regelingen-richtlijnen/protocol-incidenten-waarschuwingssysteem-financi%C3%ABle-instellingen>.

frauduleuses et des préjudices qui vont de pair.

Cependant, une base légale suffisante est nécessaire pour ce faire, comme le montre également l'examen antérieur de documents stratégiques européens. L'article 79 de la directive concernant les services de paiement – transposé dans le droit belge par l'article VII.63 du Code de droit économique et adapté depuis sur la base de l'article 94 de la deuxième directive concernant les services de paiement – définit la base légale que le législateur européen a prévue initialement à cette fin, du moins en ce qui concerne les services de paiement. Toutefois, cette base n'est pas suffisamment précise et prévoit une délégation trop large au roi. Vu la nature des données qui seraient traitées dans un système d'alerte d'incident de ce type, il convient d'être attentif au droit général relatif à la protection de la vie privée tel qu'il est prévu à l'article 22 de la Constitution. Conformément à la jurisprudence de la Cour constitutionnelle, cet article doit être compris dans le sens où « aucune ingérence des autorités dans le droit au respect de la vie privée et familiale ne [peut] intervenir si elle n'est pas prévue par des règles suffisamment précises, adoptées par une assemblée délibérante démocratiquement élue, toute ingérence dans ce droit devant répondre à un besoin social impérieux et être proportionnée à l'objectif légitime poursuivi. »³⁹ Le fondement juridique offert par la directive concernant les services de paiement n'est pas suffisamment précis pour répondre aux exigences en vertu de l'article 22 de la Constitution. Par conséquent, une nouvelle loi pouvant offrir une base légale suffisante à un tel traitement s'impose.

Il a déjà été dit précédemment que les incidents ne se limitent toutefois pas aux services de paiement offerts par les établissements de crédit, mais concernent également les crédits. Sur ce plan également, on note ces dernières années une hausse significative d'incidents, comme l'augmentation des tentatives de fraude aux fausses fiches de traitement. Dans son

gaande schadegevallen voorkomen of minstens minimaliseren.

Zoals blijkt uit de eerdere bespreking van Europese beleidsdocumenten, is hier echter een voldoende wettelijke grondslag voor nodig. Artikel 79 van de richtlijn betalingsdiensten – omgezet in Belgisch recht via artikel VII.63 Wetboek economisch recht en sindsdien aangepast in functie van artikel 94 van de tweede richtlijn betalingsdiensten – bepaalt de wettelijke grondslag die de Europese wetgever hier oorspronkelijk toe voorzien heeft, althans voor wat betreft betalingsdiensten. Deze is echter onvoldoende precies en voorziet in een te ruime delegatie aan de Koning. Gezien de aard van de gegevens die in dergelijk incidentenwaarschuwingssysteem verwerkt zouden worden, moet gelet worden op het algemene privacyrecht zoals bepaald in artikel 22 van de Grondwet. Dit artikel moet volgens de rechtspraak van het Grondwettelijk Hof begrepen worden in de zin dat “geen enkele overheidsinmenging in het recht op eerbiediging van het privéleven en het gezinsleven kan plaatsvinden dan krachtens voldoende precieze regels aangenomen door een democratisch verkozen beraadslagende vergadering, waarbij elke inmenging in dat recht dient te beantwoorden aan een dwingende maatschappelijke behoefte en evenredig dient te zijn met de nagestreefde wettige doelstelling”.⁴⁰ De rechtsgrond die de richtlijn betalingsdiensten biedt, is onvoldoende precies om aan de vereisten krachtens artikel 22 van de Grondwet te voldoen. Een nieuwe wet die voor dergelijke verwerking een voldoende wettelijke basis kan bieden, dringt zich bijgevolg op.

Eerder werd reeds aangehaald dat incidenten zich echter niet enkel beperken tot de betalingsdiensten aangeboden door de kredietinstellingen, maar ook kredieten treft. Ook hier is er de laatste jaren een significante stijging van incidenten merkbaar, zoals bijvoorbeeld toenemende fraudepogingen met valse loonfiches. In haar jaarverslag van 2020

rapport annuel 2020, la Cellule de traitement des informations financières (CTIF) fait état de 166 déclarations par des établissements de crédits hypothécaires, contre 26 déclarations en 2018.⁴¹ Dans les sociétés de crédit à la consommation, il s'agissait même d'une augmentation de 22 déclarations en 2018 à 151 déclarations en 2020, plus du sextuple.⁴² Vu le lien étroit entre les crédits et les paiements, il est dès lors conseillé d'étendre la base légale de l'échange de données que règle le présent projet de loi à la fraude au crédit.

spreekt de Cel voor Financiële Informatieverwerking (CFI) van 166 meldingen door instellingen voor hypothecair krediet, tegenover 26 meldingen in 2018.⁴³ Bij ondernemingen voor consumentenkrediet ging het zelfs om een stijging van 22 meldingen in 2018 naar 151 meldingen in 2020, meer dan een verzesvoudiging.⁴⁴ Gezien de nauwe verbondenheid van kredieten en betalingen is het daarom raadzaam om de wettelijke basis voor de uitwisseling van gegevens die dit wetsontwerp regelt uit te breiden tot kredietfraude.

III. But de la loi

Le système d'alerte d'incident a pour objectif premier de garantir l'intégrité du secteur financier, tant sur le plan de la sécurité des systèmes que sur le plan de la réputation du et de la confiance dans le secteur, en soutenant les établissements concernés dans la lutte contre l'usage abusif de services financiers, notamment en leur donnant des possibilités supplémentaires d'agir à temps.

On vise plus concrètement l'échange d'informations ou d'incidents (présumés) en lien avec la fraude, entre établissements, conformément à la présente loi. En effet, les personnes qui utilisent les services financiers de manière abusive dans un établissement tenteront probablement de le faire aussi dans d'autres établissements. Par conséquent, il est important que les établissements puissent s'alerter les uns les autres et s'échanger des données.

En identifiant plus rapidement pareils incidents, les établissements peuvent agir plus

III. Doel van de wet

Het incidentenwaarschuwingssysteem heeft als primaire doelstelling de integriteit van de financiële sector, zowel op het vlak van de veiligheid van de systemen als op het vlak van de reputatie van en het vertrouwen in de sector, te waarborgen door de betrokken instellingen te ondersteunen in de strijd tegen het oneigenlijk gebruik van financiële diensten, namelijk door hen bijkomende mogelijkheden aan te reiken om tijdig te kunnen optreden.

Meer concreet wordt de uitwisseling van (vermoedens) van fraude gerelateerde informatie of incidenten, tussen de instellingen, zoals bedoeld in deze wet, beoogd. Het is immers zo dat de personen die de financiële diensten op een oneigenlijke manier gebruiken bij een instelling dit waarschijnlijk ook bij andere instellingen zullen pogen. Bijgevolg is het van belang dat de instellingen elkaar kunnen waarschuwen en gegevens kunnen uitwisselen.

Door dergelijke incidenten spoediger te herkennen, kunnen instellingen efficiënter

⁴¹ Cellule de traitement des informations financières, « 27ème rapport d'activités 2020 », https://www.ctif-cfi.be/images/documents/French/Rapports_annuels/ra2020.pdf, 53.

⁴² *Id.*

⁴³ Cel voor Financiële Informatieverwerking, "27ste Activiteitenverslag 2020", https://www.ctif-cfi.be/website/images/NL/annual_report/jv2020.pdf, 53.

⁴⁴ *Id.*

efficacement et réduire les éventuelles conséquences préjudiciables pour les clients, les systèmes de paiement et les établissements concernés. L'enregistrement et l'échange de données concernant des incidents de ce type entraînent donc une vigilance accrue, avec laquelle le système offre aux établissements concernés la possibilité d'empêcher que certains agissements se répètent dans différents établissements concernés. Le système vise dès lors un *effet purement préventif* et n'est pas conçu pour porter atteinte aux droits des personnes (morales) concernées, comme expliqué au point VII.

La prévention, la recherche et la détection d'incidents sont en effet dans l'intérêt des citoyens, des entreprises et des autorités, ainsi que du secteur financier en tant qu'infrastructure systémique dans son ensemble. L'approche et l'évitement des incidents peuvent contribuer à préserver la continuité des services du secteur financier, comme les services de paiement et de crédit.

Pour qu'un tel échange soit opérationnel, il faut traiter des données à caractère personnel au sens du Règlement général sur la protection des données.

Cette loi n'a ni pour but, ni pour conséquence de porter atteinte à d'autres législations existantes d'application aux établissements concernés, comme par exemple le Règlement général sur la protection des données ou la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces.

IV. Constitution et fonctionnement du système d'alerte d'incidents

Le système d'alerte d'incident fonctionne comme un mécanisme d'alerte dans lequel des établissements concernés peuvent s'alerter les uns des autres à propos d'incidents concernant l'usage abusif de services de paiement et de

optreden en mogelijke nadelige gevolgen voor de cliënten, de betalingssystemen en de betrokken instellingen minimaliseren. Zo leidt de registratie en uitwisseling van gegevens inzake dergelijke incidenten tot een verhoogde waakzaamheid, waarmee het systeem de betrokken instellingen de mogelijkheid biedt om te voorkomen dat bepaalde handelingen bij verschillende betrokken instellingen herhaald worden. Het systeem beoogt dan ook een louter *preventieve werking* en is niet bedoeld om afbreuk te doen aan de rechten van de betrokken (rechts)personen zoals het onder punt VII wordt uitgelegd.

Het voorkomen, onderzoeken en opsporen van incidenten is immers in het belang van de burgers, ondernemingen en de overheid, alsook van de financiële sector als systemische infrastructuur in het geheel. Het aanpakken en vermijden van incidenten kan helpen de continuïteit van de diensten van de financiële sector te vrijwaren, zoals betaal- en kredietdiensten.

Om dergelijke uitwisseling werkbaar te laten, dienen er persoonsgegevens in de zin van de Algemene Verordening Gegevensbescherming te worden verwerkt.

Deze wet heeft niet als doel of als gevolg afbreuk te doen aan andere bestaande regelgeving van toepassing op de betrokken instellingen, zoals bijvoorbeeld de Algemene Verordening Gegevensbescherming of de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten.

IV. Samenstelling en werking van het incidentenwaarschuwingssysteem

Het incidentenwaarschuwingssysteem fungeert als een waarschuwingsmechanisme waarbij betrokken instellingen elkaar kunnen waarschuwen voor incidenten betreffende het oneigenlijk gebruik van betaal- en

crédit (par exemple, la falsification de documents comme des fiches de traitement, la fraude à l'identité, le skimming, le phishing et la tentative de fraude, etc.).

Le système est constitué d'informations qui sont directement collectées et gérées au niveau des établissements concernés individuels dans le cadre d'un incident (données d'incident) et de données limitées (données d'alerte) qui sont échangées par les établissements concernés de manière structurelle au moyen d'un registre d'alerte. Le registre d'alerte n'est pas centralisé et est géré et actualisé par chaque établissement concerné. En vue de la protection des droits et des intérêts des personnes enregistrées (tant les personnes physiques que les personnes morales), l'enregistrement dans, la consultation et la gestion de ce registre d'alerte ne sont autorisées qu'aux conditions prévues par la loi. La sécurisation du registre et la communication des informations entre des établissements concernés doivent également répondre à des exigences strictes.

V. Contenu du registre et accès aux informations

Le registre d'alerte contient exclusivement des données limitées en lien avec un incident qui s'est produit dans l'établissement concerné qui enregistre les données dans le registre, dont par exemple les données d'identification (données d'alerte). Les établissements concernés se transmettent ces données au moyen d'un canal sécurisé. L'enregistrement, la gestion et la consultation des données d'alerte ne sont possibles que par des personnes désignées spécifiquement à cette fin par chaque établissement concerné, sur la base de leurs tâches et de leur fonction. Les établissements concernés prévoient les mesures organisationnelles et techniques afin de garantir un accès limité et contrôlé.

kredietdiensten (bv. falsifiëren van documenten zoals loonfiches, identiteitsfraude, skimming, phishing, en poging tot fraude, ...).

Het systeem is samengesteld uit informatie die op het niveau van de individuele betrokken instellingen rechtstreeks verzameld en beheerd worden in het kader van een incident (incidentengegevens) en uit beperkte gegevens (waarschuwingsgegevens) die door de betrokken instellingen op structurele manier met elkaar uitgewisseld worden middels een waarschuwingsregister.

Het waarschuwingsregister is niet gecentraliseerd en wordt door elke betrokken instelling zelf beheerd en bijgewerkt. Met het oog op de bescherming van de rechten en de belangen van de geregistreerde personen (zowel natuurlijke als rechtspersonen) wordt de opname in, de raadpleging en het beheer van dit waarschuwingsregister alleen toegestaan onder de wet voorziene voorwaarden. De beveiliging van het register en de communicatie van de informatie tussen de betrokken instellingen dient ook te beantwoorden aan strikte eisen.

V. Inhoud register en toegang tot de informatie

Het waarschuwingsregister bevat uitsluitend beperkte gegevens gelinkt aan een incident dat zich heeft voortgedaan bij de betrokken instelling die de gegevens in het register opneemt, waaronder bijvoorbeeld de identificatiegegevens (waarschuwingsgegevens). Deze gegevens worden onderling door de betrokken instellingen overgemaakt middels een beveiligd kanaal. De opname, het beheer en de raadpleging van de waarschuwingsgegevens kan slechts gebeuren door personen die hiervoor specifiek door elke betrokken instelling aangesteld worden op basis van hun taken en functie. De betrokken instellingen voorzien de technische en organisatorische maatregelen om een beperkte en gecontroleerde toegang te waarborgen.

VI. Examen d'incidents et enregistrement

Afin d'éviter les enregistrements arbitraires ainsi que les enregistrements insuffisamment fondés, il est recouru à des critères objectifs sur la base desquels les personnes compétentes au sein de l'établissement concerné procéderont à une évaluation motivée pour décider si un incident s'est produit ou non et si la personne impliquée dans un incident doit être enregistrée.

Cette analyse est effectuée dans un délai raisonnable afin de donner aux personnes compétentes le temps nécessaire pour réaliser leur tâche en profondeur sur la base des éléments en leur possession.

Les personnes examinées ne sont enregistrées dans le registre d'alerte que s'il est établi dans une mesure suffisante qu'elles sont impliquées dans un incident. Si la situation est floue et/ou que le doute subsiste, il convient toujours de prendre une décision au bénéfice de la personne. Chaque établissement concerné la documentera minutieusement.

Pour ce qui est de la définition d'un incident au sens de la présente loi, on cherche en premier lieu à s'aligner sur des définitions existantes d'incidents, comme dans le cadre des services de paiement et des demandes de crédit, ainsi qu'en ce qui concerne la sécurisation des réseaux et des systèmes d'information. Ensuite, une série de typologies fréquentes sont décrites. Celles-ci comprennent des cas comme la fraude à la facture, la fraude au CEO, la fraude à l'identité et le vol d'identité, l'utilisation de documents falsifiés comme des justificatifs de revenus, la fraude au moyen du phishing et de techniques d'ingénierie sociale, avec l'intervention ou non d'une mule, ainsi que l'abus de confiance.

En outre, l'établissement concerné qui enregistre la personne communiquera les données d'alerte aux autres établissements concernés afin d'alerter ceux-ci et leur laisser la possibilité d'actualiser leurs registres d'alerte respectifs. Si l'enregistrement des données dans le registre risque de compromettre une enquête

VI. Onderzoek van incidenten en registratie

Om willekeurige registraties, alsmede registraties die onvoldoende gefundeerd zijn, te vermijden, wordt er beroep gedaan op objectieve criteria op basis van de dewelke de binnen de betrokken instelling bevoegde personen de afweging zullen maken en motiveren om te besluiten dat er zich al dan niet een incident heeft voorgedaan en of de persoon betrokken in een incident, geregistreerd dient te worden.

Deze analyse gebeurt binnen een redelijke termijn om aan de bevoegde personen de nodige tijd te geven de analyse grondig uit te voeren op basis van de elementen in hun bezit.

De onderzochte personen worden slechts opgenomen in het waarschuwingsregister indien er in voldoende mate vaststaat dat deze persoon betrokken is bij een incident. In geval van onduidelijkheid en/of twijfel dient steeds een beslissing in het voordeel van de persoon genomen te worden. Elke betrokken instellingen zal dit zorgvuldig documenteren.

Voor wat betreft de definitie van wat onder deze wet als een incident moet worden beschouwd, wordt in de eerste plaats aansluiting gezocht bij bestaande definities van incidenten, zoals in het kader rond betalingsdiensten en aanvragen kredieten alsook rond de beveiliging van netwerk- en informatiesystemen. Daarnaast worden een aantal vaak terugkomende typologieën omschreven. Deze omvatten gevallen zoals factuurfraude, CEO-fraude, identiteitsfraude en -diefstal, gebruik van vervalste stukken zoals inkomstenbewijzen, fraude door middel van phishing, en social engineering technieken, al dan niet met tussenkomst van een geldezel, alsook het misbruik van vertrouwen.

Vervolgens zal de betrokken instelling die de persoon registreert de waarschuwingsgegevens aan de andere betrokken instellingen overmaken, teneinde de andere betrokken instellingen te waarschuwen en hen de mogelijkheid te laten hun respectievelijke waarschuwingsregisters bij te werken. Indien

en cours, les établissements concernés sont dispensés de les enregistrer dans le registre d'alerte et de partager l'information.

Conformément au Règlement général sur la protection des données, les établissements concernés prévoient les mesures organisationnelles et techniques nécessaires pour garantir la sécurité et la confidentialité, pour compléter et actualiser les données à caractère personnel et pour donner aux personnes qui travaillent pour leur compte des instructions claires et une formation sur le fonctionnement du système d'alerte d'incident et sur les obligations prévues par la loi. Les établissements concernés prévoient également les contrôles et procédures internes nécessaires.

VII. Les personnes enregistrées

Les personnes enregistrées sont des personnes physiques et/ou des personnes morales impliquées dans un incident et qui ont donc manifesté des comportements ayant porté ou pouvant porter préjudice aux établissements concernés, à leurs clients et à l'intégrité des établissements concernés sur la base des critères prévus dans le présent projet.

Comme indiqué précédemment, le système sert différents intérêts. Tout d'abord, il convient de souligner l'intérêt pour les clients vu que ceux-ci sont couramment victimes de tels incidents, qui entraînent des dommages et des nuisances. Ensuite, la fraude au paiement et la fraude au crédit affectent également la confiance dans le système financier, ce qui se répercute sur le financement de l'économie. La fraude au paiement et la fraude au crédit augmentent également les coûts des services de paiement et de crédit, au détriment donc des utilisateurs de services financiers, comme les citoyens et les commerçants. Pour les services publics (en particulier les services de police et la Justice), la fraude au paiement et la fraude au crédit engendrent des frais en raison des enquêtes administratives et des instructions ainsi que des poursuites dont elles font l'objet.

het opnemen van de gegevens in het register een lopend onderzoek in het gedrang zou brengen, zijn de betrokken instellingen vrijgesteld om dit in het waarschuwingsregister op te nemen en de informatie te delen.

Conform de Algemene Verordening Gegevensbescherming voorzien de betrokken instellingen de nodige technische en organisatorische maatregelen om de beveiliging en vertrouwelijkheid te waarborgen, de persoonsgegevens bij te werken en actueel te houden en de personen die in hun opdracht werken, duidelijke instructies en opleiding te geven over de werking van het incidentenwaarschuwingssysteem en de door de wet voorziene verplichtingen. De betrokken instellingen voorzien ook in de nodige interne controles en procedures.

VII. De geregistreerde personen

De geregistreerde personen zijn natuurlijke en/of rechtspersonen die betrokken zijn in een incident en die dus gedragingen hebben vertoond die hebben geleid of kunnen leiden tot de benadeling van de betrokken instellingen, hun cliënten en de integriteit van de betrokken instellingen op basis van de criteria voorzien door dit ontwerp.

Zoals eerder aangegeven dient het systeem verscheidende belangen. Vooreerst moet gewezen worden op het belang voor de cliënten, gezien deze veelal het slachtoffer zijn van dergelijke incidenten, met schade en hinder tot gevolg. Vervolgens tast betaalfraude en kredietfraude ook het vertrouwen in het financiële systeem aan, wat doorwerkt naar de financiering van de economie. Betaalfraude en kredietfraude verhoogt ook de kosten van betaal- en kredietdiensten, en zijn aldus ook nadelig voor de gebruikers van financiële diensten, zoals burgers en handelaars. Voor de overheid (in het bijzonder de diensten van politie en justitie) veroorzaakt betaal- en kredietfraude kosten door de administratieve en gerechtelijke onderzoeken en de vervolging ervan.

Le système permet donc aux établissements concernés de prendre les mesures nécessaires afin d'intervenir *de manière préventive* et de tenter d'éviter les dommages. En d'autres termes, le système entend être un instrument préventif.

Le simple enregistrement dans le registre d'alerte n'a donc pas pour but ou pour conséquence de prendre sur la base de celui-ci des décisions qui portent préjudice aux droits de la personne enregistrée. Sur cette base, les personnes enregistrées et leurs transactions seront simplement soumises à une surveillance renforcée.

Le système ne nuit donc en aucun cas aux dispositions relatives au service bancaire de base pour les particuliers et les entreprises (Livre VII du Code de droit économique) et/ou aux dispositions du droit au crédit (Livre VII du Code de droit économique), qui incluent également les dispositions relatives à l'acceptation et au refus de crédit.

Les règles et les systèmes de protection existants destinés à garantir l'accès au système financier continuent donc de produire leur plein effet. Toutefois, le système d'alerte d'incident peut constituer une source supplémentaire dont peut se servir l'établissement concerné en appui des mesures préventives et de maîtrise des risques qu'il doit prendre pour prévenir la fraude au paiement et au crédit.

Les mesures que prendra cet établissement concerné seront donc conformes à ce que permet la réglementation actuelle. Par conséquent, la personne enregistrée conservera également tous les droits qu'accorde le droit commun pour contester la position des établissements (y compris un recours à l'Ombudsfin).

En résumé, le système sert uniquement d'alerte de risque pour les actes visés ici. Ce faisant, le système d'alerte d'incident se distingue d'une liste noire, dans laquelle le simple enregistrement pourrait avoir pour effet un refus automatique des services à la personne enregistrée. Les données mises à disposition par

Het systeem laat dus toe dat de betrokken instellingen de nodige maatregelen nemen om *preventief* in te grijpen en schade trachten te vermijden. Het systeem wil met andere woorden een preventief instrument zijn.

De loutere opname in het waarschuwingsregister heeft dus niet als doel of tot gevolg dat er op basis daarvan beslissingen worden genomen die afbreuk doen aan de rechten van de geregistreerde persoon. De geregistreerde personen en hun transacties zullen op deze basis gewoon aan een verhoogd toezicht worden onderworpen.

Het systeem doet dus geen enkele afbreuk aan de regels inzake de basisbankdienst voor particulieren en ondernemingen (Boek VII van het Wetboek economische recht) en/of aan de regels van het kredietrecht (Boek VII van het Wetboek economisch recht), waaronder ook de regels inzake de kredietaanvaarding en -weigering.

De bestaande regels en beschermingssystemen om de toegang tot het financiële systeem te garanderen blijven dus hun volle uitwerking behouden. Wel kan het incidentenwaarschuwingssysteem een bijkomende bron vormen die de betrokken instelling kan gebruiken als ondersteuning voor de preventieve en risico-beheersende maatregelen die zij dient te nemen om betaal- en kredietfraude te voorkomen.

De maatregelen die de betrokken instelling zal nemen, zullen dus conform zijn met hetgeen de huidige regelgeving toestaat. De geregistreerde persoon behoudt bijgevolg ook alle rechten die het gemeen recht toekent om de houding van de instellingen te betwisten (inclusief een beroep op Ombudsfin).

Samengevat geldt het systeem dus enkel als een risicowaarschuwing voor de hier bedoelde handelingen. Hiermee onderscheidt het incidentenwaarschuwingssysteem zich van een zwarte lijst, waar de loutere registratie tot gevolg zou kunnen hebben dat de geregistreerde persoon diensten automatisch geweigerd

le système servent uniquement à étayer l'évaluation des risques existante dans le cadre de l'offre de biens et services sans porter préjudice aux obligations en vigueur, concernant le service bancaire de base, par exemple.

worden. De door het systeem beschikbaar gestelde gegevens dienen enkel ter ondersteuning van de reeds bestaande risico-inschatting in het kader van het aanbod van goederen en diensten zonder hierbij afbreuk te doen aan geldende verplichtingen, zoals bijvoorbeeld inzake de basisbankdienst.

VIII. Droits des personnes enregistrées

Indépendamment des droits fondés sur le Règlement général sur la protection des données (voir point XI), la personne enregistrée se voit accorder un droit à la contradiction. Celui-ci laisse à la personne enregistrée la possibilité de réagir à un enregistrement, de nouveaux éléments susceptibles d'influencer la décision de procéder à l'enregistrement pouvant également être apportés. Cela permet également de reconnaître si une personne enregistrée qui, sur la base des éléments en possession de l'établissement concerné, semblait à première vue être l'auteur d'un incident, mais qui doit plutôt être considérée comme une victime, par exemple parce qu'elle a été utilisée à son insu comme mule.

En outre, les autres droits de la personne enregistrée restent intégralement d'application, comme le droit de s'adresser au service de médiation compétent, Ombudsfin pour le secteur financier, ou les procédures en vigueur dans le cadre du droit à la protection des données à déposer plainte auprès de l'Autorité de protection des données et la procédure judiciaire.

IX. Obligations des établissements concernés

Comme indiqué au point VI, l'établissement concerné – qui décide de procéder à l'enregistrement – porte la responsabilité finale de cette décision. Chaque établissement concerné porte en outre une responsabilité vis-à-vis des données reçues via le système. Tous deux ont l'obligation de tenir à jour les données introduites, ou les alertes de risque reçues, en

VIII. Rechten van de geregistreerde personen

Onafgezien van de rechten op basis van de Algemene Verordening gegevensbescherming (zie punt XI), wordt aan de geregistreerde personen een recht op tegenspraak toegekend. Dit laat aan de geregistreerde persoon de mogelijkheid om te reageren op een registratie, waarbij ook nieuwe elementen kunnen worden aangedragen die de beslissing tot registratie kunnen beïnvloeden. Dit laat ook toe om te erkennen wanneer een geregistreerde persoon die, op basis van de elementen in het bezit van de betrokken instelling, in eerste instantie de dader van een incident leek, toch eerder als slachtoffer gekenmerkt moet worden, bijvoorbeeld doordat deze onbewust als geldezel gebruikt werd.

Daarnaast blijven de overige rechten van de geregistreerde persoon, zoals het recht zich te wenden tot de bevoegde ombudsdienst, voor de financiële sector Ombudsfin, of de binnen het gegevensbeschermingsrecht geldende procedures van het indienen van een klacht bij de Gegevensbeschermingsautoriteit en de gerechtelijke procedure, onverkort gelden.

IX. Verplichtingen van de betrokken instellingen

Zoals onder punt VI is aangegeven, draagt de betrokken instelling - die beslist tot registratie over te gaan - de eindverantwoordelijkheid voor die beslissing. Elke betrokken instelling draagt bovendien een verantwoordelijkheid voor de via het systeem ontvangen gegevens. Beide zijn verplicht om de ingevoerde gegevens, dan wel de ontvangen risicowaarschuwingen, actueel te

procédant à des modifications, à des réconciliations et à des contrôles.

houden door wijzigingen, reconciliaties en controles uit te voeren.

X. Délai de conservation

Le délai de conservation des données dans le registre d'alerte est fixé à dix ans, à compter de la date d'enregistrement. À l'expiration du délai de conservation, les données enregistrées sont supprimées automatiquement et définitivement. L'objectif recherché avec ce délai de conservation de dix ans est de s'aligner sur les délais de conservation habituels au sein du secteur pour les données en matière de fraude.

X. Bewaartermijn

De bewaartermijn van de gegevens in het waarschuwingsregister wordt bepaald op tien jaar, te rekenen vanaf de datum van registratie. Na het verstrijken van de bewaartermijn worden de geregistreerde gegevens automatisch en definitief verwijderd. Met de bewaartermijn van tien jaar wordt aansluiting gezocht bij de binnen de sector gangbare bewaartermijnen inzake fraudegegevens.

XI. Traitement de données à caractère personnel

La protection de la vie privée exige que le fondement légal pour ce partage d'informations comporte un certain nombre d'éléments essentiels incontestables.⁴⁵ Ce projet vise à définir les éléments essentiels suivants concernant le système d'alerte d'incident :

- La licéité et la finalité du traitement de données ;
- La ou les personnes concernées ;
- Les cas et les conditions d'enregistrement ;
- Les catégories de données à traiter ;
- Les droits de la personne concernée ;
- Les obligations des établissements concernés.

XI. Verwerking van persoonsgegevens

De bescherming van de persoonlijke levenssfeer vergt dat de wettelijke grondslag voor dergelijke informatiedeling onbetwistbaar een aantal essentiële elementen moet omvatten.⁴⁶ Dit ontwerp beoogt de volgende essentiële elementen aangaande het incidentenwaarschuwingssysteem vast te stellen:

- De rechtmatigheid en doelstelling van de gegevensverwerking;
- De betrokkene(n);
- De gevallen en voorwaarden van registratie;
- Categorieën van te verwerken gegevens;
- De rechten van de betrokkene;
- Verplichtingen van de betrokken instellingen.

⁴⁵ Des indications quant à ce qu'il convient de considérer comme des éléments essentiels figurent notamment au considérant 46 du Règlement général sur la protection des données ainsi que dans la jurisprudence de la Cour constitutionnelle.

⁴⁶ Indicaties voor wat als dergelijke essentiële elementen beschouwd worden, kunnen worden teruggevonden in onder meer overweging 46 van de Algemene Verordening Gegevensbescherming, alsook in de rechtspraak van het Grondwettelijk Hof.

Ces éléments sont commentés plus en détail ici.

Deze elementen worden hier nader toegelicht.

Vu que le système d'alerte d'incident peut avoir un impact sur la vie privée, les traitements et échanges de données doivent être clairement délimités et encadrés par la loi.

Gelet op het feit dat het incidentenwaarschuwingssysteem een impact kan hebben op de persoonlijke levenssfeer is het noodzakelijk dat de gegevensverwerkingen en -uitwisseling duidelijk omlijnd en wettelijk omkaderd worden.

Un traitement de données à caractère personnel doit reposer sur un des fondements contenus à l'article 6 du Règlement général sur la protection des données. Ce projet de loi impose aux établissements concernés une obligation légale de traiter les données à caractère personnel dans le système d'alerte d'incident. Conformément à cette obligation, ce traitement se fondera sur l'article 6, paragraphe 1, c), du Règlement général sur la protection des données. Celui-ci précise, en effet, que le traitement est autorisé lorsqu'il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis. Cela vaut également pour l'enregistrement des données de la victime d'un incident, la finalité primaire de l'enregistrement étant la protection de la victime.

Een verwerking van persoonsgegevens dient te berusten op een van de grondslagen vervat in artikel 6 van de Algemene Verordening Gegevensbescherming. Met dit wetsontwerp wordt de betrokken instellingen een wettelijke verplichting tot het verwerken van persoonsgegevens in het incidentenwaarschuwingssysteem opgelegd. Ingevolge deze verplichting zal die verwerking gebaseerd zijn op artikel 6, eerste lid, c van de Algemene Verordening Gegevensbescherming als grondslag. Deze stelt immers dat een verwerking toegelaten is wanneer deze noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust. Dit geldt ook voor de registratie van de gegevens van een slachtoffer van een incident, waarbij het primaire doel van de registratie de bescherming van het slachtoffer beoogt.

Afin de satisfaire à l'exigence de transparence et de prévisibilité, les finalités pour lesquelles ces données à caractère personnel seront traitées doivent être énumérées de manière explicite et restrictive. Le principe est que les données à caractère personnel seront traitées exclusivement pour les finalités spécifiques et bien définies dans le présent projet de loi et pour autant que ce soit nécessaire pour pouvoir atteindre les finalités préalablement définies. Ainsi, le projet de loi ne permet pas le traitement de données à caractère personnel pour d'autres finalités que celles qui y sont définies. À titre d'exemple, les données enregistrées dans le système d'alerte d'incident ne pourront être utilisées pour proposer des services commerciaux.

Om te voldoen aan de vereiste van transparantie en voorzienbaarheid is het noodzakelijk dat de doelstellingen waarvoor die persoonsgegevens zullen worden verwerkt uitdrukkelijk en op limitatieve wijze worden opgesomd. Als uitgangspunt geldt dat persoonsgegevens uitsluitend zullen worden verwerkt voor de specifieke en welomschreven doeleinden die in het voorliggend wetsontwerp omschreven worden en voor zover dit noodzakelijk is om die vooropgestelde doeleinden te kunnen bereiken. Het ontwerp van wet biedt aldus geen mogelijkheid voor de verwerking van persoonsgegevens voor andere doeleinden dan deze hierin omschreven. Zo zal bijvoorbeeld voor het aanbieden van commerciële diensten geen gebruik kunnen worden gemaakt van de in het incidentenwaarschuwingssysteem opgenomen gegevens.

Pour chaque catégorie de données, il convient de justifier si l'enregistrement est pertinent, approprié et proportionnel pour les finalités du système d'alerte d'incident qui ont été définies. Pour satisfaire à cette obligation, le projet de loi impose l'utilisation de champs prédéfinis qui peuvent être complétés. Les catégories de données supplémentaires sont par conséquent exclues du traitement.

L'objectif limité du traitement de données à caractère personnel dans le cadre du système d'alerte d'incident implique également qu'il n'est pas prévu de transmettre les données traitées à d'autres acteurs que les établissements concernés. Le présent projet de loi sert donc un intérêt social plus large. Il importe à cet égard, comme exigé, que les données à traiter restent limitées à ce qui est strictement nécessaire dans le cadre de la préservation de cet intérêt. Le délai de conservation est imposé par la loi.

De l'attention est également prêtée aux intérêts de la personne enregistrée. Outre l'enregistrement des données à caractère personnel de celle-ci, il convient, en effet, de prendre en considération le fait qu'un tel enregistrement peut avoir une connotation négative. C'est la raison pour laquelle l'enregistrement ne doit pas aller au-delà de ce qui est absolument nécessaire au maintien des intérêts précités. Par ailleurs, les droits de la personne concernée définis dans le Règlement général sur la protection des données restent d'application. La personne concernée pourra exercer ses droits auprès de l'établissement concerné qui a initialement procédé à l'enregistrement. La transparence est présumée par la mise à disposition de la personne concernée d'informations concernant l'existence et le fonctionnement du système. La personne enregistrée est également informée de manière spécifique de l'enregistrement de ses données dans le système. Enfin, des conditions claires sont posées en ce qui concerne les mesures techniques et organisationnelles destinées à protéger les données à caractère personnel de la personne enregistrée.

Voor elke gegevenscategorie moet worden verantwoord of de registratie relevant, passend en proportioneel is voor de omschreven doeleinden van het incidentenwaarschuwingssysteem. Om hieraan tegemoet te komen, legt dit wetsontwerp het gebruik op van vooraf bepaalde velden die kunnen worden ingevuld. Bijkomende gegevenscategorieën worden bijgevolg uitgesloten van de verwerking.

De beperkte doelstelling van de verwerking van persoonsgegevens in kader van het incidentenwaarschuwingssysteem houdt ook in dat er niet voorzien wordt in de doorgifte van de verwerkte gegevens aan andere actoren dan de betrokken instellingen. De voorliggende verwerking dient ook een ruimer maatschappelijk belang dient. Van belang hierbij is, zoals vereist, dat de te verwerken gegevens beperkt blijven tot wat strikt noodzakelijk is in het kader van de vrijwaring van dit belang. De bewaringstermijn wordt opgelegd door de wet.

Ook wordt aandacht besteed aan de belangen van de geregistreerde persoon. Naast de registratie van diens persoonsgegevens moet immers in acht genomen worden dat dergelijke registratie een negatieve bijklank kan hebben. De registratie mag daarom niet verder gaan dan absoluut noodzakelijk voor de handhaving van de voormelde belangen. Verder blijven de rechten van de betrokkene zoals bepaald in de Algemene Verordening Gegevensbescherming gelden. De betrokkene zal zijn rechten bij de betrokken instelling die initieel is overgegaan tot registratie kunnen uitoefenen. De transparantie wordt vooropgesteld door aan de betrokken personen informatie over het bestaan en de werking van het systeem ter beschikking te stellen. De geregistreerde persoon wordt eveneens specifiek ingelicht over de opname van zijn gegevens in het systeem. Tenslotte worden duidelijke voorwaarden gesteld wat betreft de technische en organisatorische maatregelen die de persoonsgegevens van de geregistreerde persoon moeten beschermen.

Conformément à l'article 23.1, d) et i), du Règlement général sur la protection des données, les droits de la personne concernée, sur la base des articles 12 à 22 du Règlement général sur la protection des données, ne s'appliqueront pas lorsqu'ils risquent d'entraver la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière et/ou l'exécution de sanctions pénales, voire de compromettre la protection de la victime. Cette dispense s'applique uniquement à ces cas spécifiques.

Les établissements concernés sont, chacun, le responsable du traitement pour leur système. Ils reconnaissent que les données à caractère personnel enregistrées dans le cadre du système d'alerte d'incident sont strictement confidentielles et doivent être traitées comme telles. Afin de satisfaire à cet aspect, chaque établissement concerné limite l'accès aux données à celles qui sont nécessaires au fonctionnement du système.

Seules les personnes désignées, disposant d'un accès au système d'alerte d'incident, pourront prendre connaissance du contenu de l'enregistrement. Le *data protection officer* désigné en interne, ou délégué à la protection des données, veille au respect des exigences techniques et organisationnelles qui découlent du Règlement général sur la protection des données. L'implication de cette personne – ainsi que l'implication éventuelle du service de médiation compétent, de l'Autorité de protection des données ou du tribunal – offre une garantie contre l'utilisation abusive du système d'alerte d'incident par les établissements concernés.

Conform artikel 23.1, d) en i) Algemene Verordening Gegevensbescherming zullen de rechten van de betrokkene op basis van artikelen 12 tot 22 van de Algemene Verordening Gegevensbescherming niet van toepassing zijn wanneer het de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten en/of de tenuitvoerlegging van straffen kunnen verhinderen of zelfs de bescherming van het slachtoffer in het gevaar kunnen brengen. Deze vrijstelling geldt enkel voor deze specifieke gevallen.

De betrokken instellingen zijn elk de verwerkingsverantwoordelijke voor hun systeem. Zij erkennen dat de persoonsgegevens die in het kader van het incidentenwaarschuwingssysteem worden geregistreerd, strikt vertrouwelijk zijn en als zodanig moeten worden behandeld. Om hieraan tegemoet te komen beperkt iedere betrokken instelling de toegang tot de gegevens tot degenen die noodzakelijk zijn voor de werking van het systeem.

Enkel de aangewezen personen met toegang tot het incidentenwaarschuwingssysteem zullen kunnen kennisnemen van de inhoud van de registratie. De intern aangestelde *data protection officer*, oftewel de functionaris voor gegevensbescherming, waakt over de naleving van de organisatorische en technische vereisten die volgen uit de Algemene Verordening Gegevensbescherming. De betrokkenheid van deze persoon – alsook de mogelijke betrokkenheid van de bevoegde ombudsdienst, de Gegevensbeschermingsautoriteit of het gerecht – biedt waarborg tegen het misbruik van het incidentenwaarschuwingssysteem door de betrokken instellingen.

COMMENTAIRE DES ARTICLES

Section 1^{re}. Dispositions générales

Article 1^{er}. Fondement constitutionnel

Le présent article précise que le projet de loi règle une matière visée à l'article 74 de la Constitution.

TOELICHTING BIJ DE ARTIKELEN

Afdeling 1. Algemene bepalingen

Artikel 1. Grondwettelijke grondslag

In dit artikel wordt gepreciseerd dat het wetsontwerp een aangelegenheid regelt als bedoeld in artikel 74 van de Grondwet.

Article 2. Définitions

Le présent article établit les définitions des notions utilisées dans le présent projet.

Les nouvelles notions insérées par le présent article concernent le système même, ainsi que les incidents dont les données concernées seraient intégrées dans le système. La portée précise de ces notions est définie plus avant dans les articles suivants.

Artikel 2. Definities

Dit artikel bepaalt de definities van de in dit ontwerp gehanteerde begrippen.

De nieuwe begrippen ingevoerd bij dit artikel betreffen het systeem zelf, alsook de incidenten van welke de betrokken gegevens in het systeem opgenomen zouden worden. De precieze draagwijdte van deze begrippen wordt in verdere artikelen nader afgebakend.

Section 2. Création du système d’alerte d’incidents

Article 3. But du système

Les objectifs de l’échange d’informations sont définis de manière exhaustive dans le présent article. Du point de vue de la protection des données à caractère personnel, cela permet de protéger les données de possibles traitements ultérieurs qui ne correspondent pas aux objectifs du système.

Afdeling 2. Oprichting van het Incidentenwaarschuwingssysteem

Artikel 3. Doel van het systeem

De doelstellingen van de uitwisseling van informatie worden in dit artikel exhaustief bepaald. Vanuit persoonsgegevensbescherming laat dit toe de gegevens te beschermen tegen mogelijke verdere verwerkingen die niet overeenstemmen met de doelstellingen van het systeem.

Article 4. Description du système

Le présent article prévoit la création du système d’alerte d’incidents auprès des établissements concernés. Le système comporte, d’une part, des informations directement collectées par chaque établissement individuel concerné dans le cadre d’un incident, et, d’autre part, des informations limitées échangées entre les établissements concernés. Le registre d’alerte concerne des données limitées, partagées de manière structurelle avec les établissements concernés.

Artikel 4. Beschrijving van het systeem

Dit artikel voorziet in de oprichting van het incidentenwaarschuwingssysteem bij de betrokken instellingen. Het systeem bestaat, enerzijds, uit informatie die rechtsreeks door elke individuele betrokken instelling verzameld wordt in het kader van een incident, en anderzijds, uit beperkte tussen de betrokken instellingen uitgewisselde informatie. Het waarschuwingsregister betreft beperkte gegevens die op structurele manier gedeeld worden met de betrokken instellingen.

Section 3. Incidents et traitement

Article 5. Incidents

Le présent article énumère ce qui peut être considéré comme un incident au sens de la

Afdeling 3. Incidenten en behandeling

Artikel 5. Incidenten

Dit artikel geeft een opsomming van wat kan beschouwd worden als een incident in de zin van

présente loi. Les données afférentes à un incident ne peuvent être traitées dans le système que s'il est question d'un incident en vertu du présent article.

En outre, une obligation de motivation est imposée à titre de mesure supplémentaire afin d'éviter des décisions subjectives d'enregistrement. Des critères objectifs sont établis afin de guider cette prise de décision.

Il est souligné que le système d'alerte d'incidents ne vise pas à faire office de liste noire dans le cadre de laquelle le simple enregistrement impliquerait que la personne enregistrée soit automatiquement exclue du système financier.

deze wet. Enkel wanneer sprake is van een incident krachtens dit artikel kunnen de hieraan gerelateerde gegevens verwerkt worden in het systeem.

Bovendien wordt een motiveringsplicht opgelegd als bijkomende maatregel om subjectieve beslissingen tot registratie te vermijden. Er worden objectieve criteria vastgelegd om deze besluitvorming te sturen.

Er wordt benadrukt dat het incidentenwaarschuwingssysteem geen zwarte lijst beoogt te zijn, waar de loutere registratie tot gevolg zou kunnen hebben dat de geregistreerde persoon automatisch van het financieel systeem uitgesloten zou worden.

Article 6. Description des données d'alerte

Le présent article décrit la catégorie et le type de données (à caractère personnel) de personnes physiques et de personnes morales qui sont enregistrées dans le registre d'alerte. Cette description est exhaustive et interdit, par conséquent, le traitement d'autres données. Cette description de données peut être complétée/adaptée par le Roi, à la suite d'éventuelles évolutions sociales et technologiques, à l'exception des données à caractère personnel.

Artikel 6. Beschrijving van de waarschuwingsgegevens

Dit artikel omschrijft de categorie en het type (persoons)gegevens van natuurlijke personen en rechtspersonen die worden opgenomen in het waarschuwingsregister. Deze omschrijving is exhaustief en verbiedt bijgevolg de verwerking van andere gegevens. Ingevolge mogelijke maatschappelijke en technologische evoluties kan deze omschrijving van gegevens door de Koning aangevuld/aangepast worden, met uitzondering van persoonsgegevens.

Article 7. Délai de conservation

Le présent article détermine le délai pendant lequel les données d'alerte peuvent être conservées.

Artikel 7. Bewaartermijn

Dit artikel bepaalt de termijn binnen dewelke de waarschuwingsgegevens bewaard kunnen worden.

Section 4. Gestion du et accès au système et échange de données d'alerte

Afdeling 4. Beheer van en toegang tot het systeem en uitwisseling van waarschuwingsgegevens

Article 8. Responsabilité vis-à-vis du système

Artikel 8. Verantwoordelijkheid voor het systeem

Le présent article précise les responsabilités

Dit artikel preciseert de verantwoordelijkheden

dans le cadre de ce système. Plus particulièrement en ce qui concerne la protection des données à caractère personnel, le présent article désigne le responsable du traitement pour les données à caractère personnel enregistrées dans le système.

Le principe est que l'établissement concerné qui procède à l'enregistrement des données liées à des incidents est désigné en tant que responsable du traitement. Chacun des établissements concernés prendra les mesures organisationnelles et techniques adéquates afin de garantir l'utilisation correcte et la sécurisation du système.

Articles 9 et 10. Accès, gestion et échange d'informations

Il convient de définir la manière dont les établissements concernés enregistrent les données dans le registre d'alerte et comment ces données peuvent être partagées avec les autres établissements concernés, le principe de base étant que l'accès au registre même doit, en principe, être limité aux personnes désignées par l'établissement concerné.

Il convient de définir précisément quelles personnes peuvent, pour le compte de l'établissement concerné, prendre connaissance du contenu des données d'alerte et à quelle condition les informations peuvent être partagées. Ainsi, la personne compétente ne pourra, par exemple, être informée de l'existence d'un enregistrement dans le registre d'alerte que dans l'exercice de ses tâches.

Pour ce qui concerne les aspects techniques et sécuritaires de l'échange de données entre les établissements concernés, le présent article prévoit l'obligation pour ces derniers de conclure un protocole. Compte tenu des évolutions technologiques et de la flexibilité que de telles adaptations peuvent exiger, il n'est pas indiqué de prévoir cet aspect dans la loi même.

in het kader van dit systeem. Meer bepaald op het vlak van de persoonsgegevensbescherming duidt dit artikel de verwerkingsverantwoordelijke aan voor de in het systeem opgenomen persoonsgegevens.

Als uitgangspunt wordt de betrokken instelling welke tot registratie overgaat van de gegevens gerelateerd aan incidenten aangeduid als verwerkingsverantwoordelijke. Elk van de betrokken instellingen zal de passende organisatorisch en technische maatregelen nemen om het correct gebruik en de beveiliging van het systeem te waarborgen.

Artikelen 9 en 10. Toegang, beheer en uitwisseling van informatie

Er dient te worden bepaald hoe de gegevens in het waarschuwingsregister worden geregistreerd door de betrokken instellingen en op welke manier deze gegevens met de andere betrokken instellingen gedeeld kunnen worden, met als uitgangspunt dat de toegang tot het register zelf in principe beperkt dient te worden tot de door de betrokken instelling aangeduide personen.

Er moet nauwkeurig omschreven worden welke personen, in opdracht van de betrokken instelling, kennis kan nemen van de inhoud van de waarschuwingsgegevens en aan welke voorwaarde de informatie gedeeld kan worden. Zo zal bijvoorbeeld de bevoegde persoon enkel in de uitoefening van zijn of haar taken in kennis gesteld kunnen worden van het bestaan van een registratie in het waarschuwingsregister.

Voor wat de technische en veiligheidsaspecten van de uitwisseling van gegevens tussen de betrokken instellingen betreft, voorziet dit artikel de verplichting voor de betrokken instellingen om een Protocol te sluiten. Gelet op de technologische evoluties en de flexibiliteit die dergelijke aanpassingen kunnen vergen, is het niet aangewezen om dit in de wet zelf te voorzien.

**Section 5. Informations concernant le système
d'alerte d'incidents et communication
concernant l'enregistrement**

Article 11. Informations concernant le système

Le présent article impose, par ailleurs, également une obligation de transparence. Les établissements concernés doivent mettre à la disposition des personnes concernées des informations relatives à l'existence et au fonctionnement du système.

**Article 12. Communication concernant
l'enregistrement**

Le présent article prévoit que l'enregistrement dans le registre d'alerte est porté à la connaissance de la personne enregistrée par l'établissement concerné qui procède à l'enregistrement, sauf si cette notification compromet la détection d'infractions pénales et/ou les poursuites en la matière, voire si elle compromet la protection de la victime dans le cadre d'une enquête de police et/ou d'une instruction.

**Section 6. Droits de la personne en rapport
avec l'incident**

Article 13. Droit à la contradiction

La personne enregistrée a la possibilité d'exercer son droit à la contradiction à l'encontre de l'enregistrement effectué par l'établissement concerné, à compter de la notification de l'enregistrement, et ce, à l'aide du formulaire disponible publiquement. Dans ce cadre, la personne enregistrée peut également avancer de nouveaux éléments susceptibles d'influer sur la décision d'enregistrement. Après réception du formulaire, l'établissement concerné vérifiera si, sur la base des informations transmises ~~et~~ ~~réponse~~ et d'éventuels nouveaux éléments, les critères permettant l'enregistrement sont toujours remplis et si l'enregistrement a été suffisamment motivé. Cette procédure laisse intacts les autres droits de la personne

**Afdeling 5. Informatie over het
Incidentenwaarschuwingssysteem en
bekendmaking registratie**

Artikel 11. Informatie over het systeem

Dit artikel legt daarnaast ook een transparantieplicht op. De betrokken instellingen dienen informatie over het bestaan en de werking van het systeem aan de betrokken personen ter beschikking te stellen.

Artikel 12. Bekendmaking van de registratie

Dit artikel voorziet in de bekendmaking van de registratie in het waarschuwingsregister aan de geregistreerde persoon door de betrokken instelling die tot de opname overgaat behoudens indien deze bekendmaking de opsporing en/of de vervolging van strafbare feiten of zelfs de bescherming van het slachtoffer in het kader van een politie- en/of gerechtelijk onderzoek in het gedrang brengt.

**Afdeling 6. Rechten van de aan het incident
gerelateerde persoon**

Artikel 13. Recht op tegenspraak

De geregistreerde persoon krijgt de mogelijkheid om tegenspraak uit te oefenen tegen de registratie door de betrokken instelling vanaf de bekendmaking van de opname aan de hand van een publiek toegankelijk standaardformulier. Hierbij kan de geregistreerde persoon ook nieuwe elementen aandragen die de beslissing tot registratie kunnen beïnvloeden. De betrokken instelling zal na ontvangst van het formulier nagaan of met de overgemaakte informatie en eventuele nieuwe elementen de criteria voor de registratie nog steeds vervuld zijn en of de opname voldoende gemotiveerd werd. Deze procedure laat onverkort de overige rechten van de geregistreerde persoon.

enregistrée.

Article 14. Droits fondés sur le Règlement général sur la protection des données

Les personnes physiques liées à l'incident sont des personnes concernées au sens du Règlement général sur la protection des données. Elles disposent, dès lors, des droits prévus dans le règlement. Toutefois s'il s'avère que l'exercice de ces droits comporte un risque d'entraver la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière et/ou l'exécution de sanctions pénales, et/ou un risque de compromettre la protection de la victime, ceux-ci ne seront pas d'application conformément à l'article 23.1, d) et i), du Règlement général sur la protection des données. ~~ne risque pas~~

Artikel 14. Rechten op basis van de Algemene Verordening Gegevensbescherming

De aan het incident gerelateerde natuurlijke personen zijn betrokken personen in de zin van de Algemene Verordening Gegevensbescherming. Bijgevolg beschikken zij over de rechten zoals voorzien in de verordening. Indien blijkt dat de uitoefening van deze rechten, de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten en/of de tenuitvoerlegging van straffen kan verhinderen en/of de bescherming van het slachtoffer in het gevaar kan brengen, zullen deze rechten niet van toepassing zijn conform artikel 23.1, d) en i) Algemene Verordening Gegevensbescherming.

Section 7. Litiges

Article 15. Litiges

Outre les mécanismes de défense et les droits prévus par la loi, les personnes enregistrées peuvent également introduire une plainte auprès d'Ombudsfin.

Afdeling 7. Geschillen

Artikel 15. Geschillen

De geregistreerde personen kunnen naast de verdedigingsmechanismen en rechten voorzien door de wet, ook klacht indienen bij Ombudsfin.

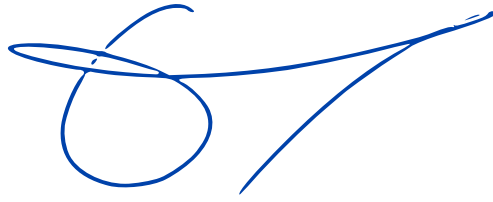
Le Ministre des Finances,

De Minister van Financiën

VINCENT VAN PETEGHEM

Le Ministre de la Justice,

De Minister van Justitie,

A handwritten signature in blue ink, consisting of a large, stylized 'V' followed by a horizontal line and a diagonal stroke.

VINCENT VAN QUICKENBORNE