DOC 56 **0173/002**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

4 juni 2025

WETSVOORSTEL

betreffende de veiligheid in recreatiedomeinen

Advies van de Gegevensbeschermingsautoriteit

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

4 juin 2025

PROPOSITION DE LOI

relative à la sécurité dans les domaines récréatifs

Avis de l'Autorité de protection des données

Zie:

Doc 56 **0173/ (B.Z. 2024)**:
001: Wetsvoorstel van de heer Demon c.s.

Voir:

Doc 56 **0173/ (S.E. 2024)**:
001: Proposition de loi de M. Demon et consorts.

N-VA	:	*Nieuw-Vlaamse Alliantie*
VB	:	*Vlaams Belang*
MR	:	*Mouvement Réformateur*
PS	:	*Parti Socialiste*
PVDA-PTB	:	*Partij van de Arbeid van België – Parti du Travail de Belgique*
Les Engagés	:	*Les Engagés*
Vooruit	:	*Vooruit*
cd&v	:	*Christen-Democratisch en Vlaams*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
Open Vld	:	*Open Vlaamse liberalen en democraten*
DéFI	:	*Démocrate Fédéraliste Indépendant*
ONAFH/INDÉP	:	*Onafhankelijk-Indépendant*

Afkorting bij de nummering van de publicaties:		*Abréviations dans la numérotation des publications:*	
DOC 56 0000/000	*Parlementair document van de 56e zittingsperiode + basisnummer en volgnummer*	*DOC 56 0000/000*	*Document de la 56e législature, suivi du numéro de base et numéro de suivi*
QRVA	*Schriftelijke Vragen en Antwoorden*	*QRVA*	*Questions et Réponses écrites*
CRIV	*Voorlopige versie van het Integraal Verslag*	*CRIV*	*Version provisoire du Compte Rendu Intégral*
CRABV	*Beknopt Verslag*	*CRABV*	*Compte Rendu Analytique*
CRIV	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toespraken (met de bijlagen)*	*CRIV*	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*
PLEN	*Plenum*	*PLEN*	*Séance plénière*
COM	*Commissievergadering*	*COM*	*Réunion de commission*
MOT	*Moties tot besluit van interpellaties (beigekleurig papier)*	*MOT*	*Motions déposées en conclusion d'interpellations (papier beige)*

Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 06/2025 van 30 januari 2025

Betreft: Advies m.b.t. een wetsvoorstel *betreffende de veiligheid in recreatiedomeinen* (de artikelen 14, 16, 20, 21, 25, 32, 33, 34) (CO-A-2024-282)

Originele versie

Inleiding

Het ter advies voorgelegde wetsontwerp *betreffende de veiligheid in recreatiedomeinen* situeert zich binnen de aanpak en afhandeling van onaanvaardbaar gedrag in en rond recreatiedomein, en stelt een (wettelijk) kader vast voor de sanctionering in dat verband, gebaseerd op de wet van 21 december 1998 *betreffende de veiligheid bij voetbalwedstrijden.*

Hoewel de Autoriteit in beginsel begrip heeft voor de onderhavige problematiek, stelt zij niettemin vast dat een aantal wijzigingen aan het ontwerp zich opdringen.

De belangrijkste opmerking in dat verband betreft de noodzaak om de organisatorische en technische modaliteiten van de toegangscontrole (en het 'hit'/ 'no-hit' systeem) reeds uitdrukkelijk vast te stellen in het ontwerp, op een zodanige wijze dat er geen koppeling plaatsvindt tussen de feitelijke identiteitscontrole en het centraal sanctiebestand en dat het voor de domeinuitbaters en diens aangestelden geenszins mogelijk is om rechtstreeks zicht te hebben op de (persoons)gegevens die geregistreerd zijn in dat bestand.

Daarnaast formuleert de Autoriteit nog een aantal bemerkingen inzake de noodzaak om de hoedanigheid van de domeinuitbaters vast te stellen, de te hanteren definitie van bepaalde gegevenscategorieën en (het moment van aanvang van) de bewaartermijnen van de persoonsgegevens.

Tot slot stelt de Autoriteit zich belangrijke vragen inzake de proportionaliteit en de noodzakelijkheid van de vastgestelde maximale perimeter rond recreatiedomeinen en de mogelijkheid om daarbinnen verregaand op te treden jegens personen.

Voor normatieve teksten die uitgaan van de federale overheid, het Brussels Hoofdstedelijk Gewest en de Gemeenschappelijke Gemeenschapscommissie zijn de adviezen in principe zowel in het Nederlands als in het Frans beschikbaar op de website van de Autoriteit. De 'Originele versie' is de versie die collegiaal gevalideerd werd.

Voor een exhaustieve oplijsting van de opmerkingen verwijst de Autoriteit naar het dispositief.

De Autorisatie- en Adviesdienst van de Gegevensbeschermingsautoriteit (hierna: de Autoriteit), aanwezig: mevrouw Cédrine Morlière, mevrouw Nathalie Ragheno en mevrouw Griet Verhenneman en de heren Yves-Alexandre de Montjoye, Bart Preneel en Gert Vermeulen;

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit,* inzonderheid op artikelen 23 en 26 (hierna: "WOG");

Gelet op artikel 43 van het Reglement van interne orde volgens hetwelk de beslissingen van de autorisatie- en adviesdienst bij meerderheid van stemmen worden aangenomen;

Gelet op de 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* (hierna: "AVG");

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* (hierna: "WVG");

Gelet op het verzoek om advies van de heet Peter De Roover, Voorzitter van de Kamer van volksvertegenwoordigers, (hierna: "de aanvrager"), ontvangen op 4 november 2024

Gelet op de bespreking ter zitting van de Autoriteit van 23 januari 2025, alwaar werd besloten tot voortzetting bij wijze van schriftelijke procedure;

Brengt op 30 januari 2025, bij wijze van schriftelijke procedure, het volgend advies uit:

I. VOORWERP VAN DE ADVIESAANVRAAG

1. Op 4 november 2024 verzocht de aanvrager het advies van de Autoriteit met betrekking tot de artikelen 14, 16, 20 – 21, 25 en 32 – 34 van het wetsvoorstel *betreffende de veiligheid in recreatiedomeinen* (hierna: "het ontwerp").

2. Dit wetsvoorstel neemt gedeeltelijk de tekst over van de voorstellen DOC 53 2224/001, DOC 54 373/001 en DOC 55 3434/001, in het bijzonder rekening houdend met de adviezen die reeds werden ingewonnen over voorstel DOC 55 3434/001. In dit verband moet ook gewezen worden

op het advies nr. 18/2023[1] van de Autoriteit met betrekking tot een wetsvoorstel *tot wijzing van de Nieuwe Gemeentewet houdende het faciliteren van een nationaal toegangsverbod voor recreatiedomeinen*, met als voornaamste punten van kritiek dat er geen duidelijke afbakening is van het begrip 'recreatiedomein', dat het onduidelijk is onder welke voorwaarden en in welke omstandigheden een persoon gesanctioneerd kan worden[2], dat de rol van de uitbaters van recreatiedomeinen inzake sanctionering en controle van domein- en perimeterverboden onvoldoende omkaderd is en dat er te weinig maatregelen zijn genomen om de naleving van het recht op gegevensbescherming te verzekeren. In dit advies onderzoekt de Autoriteit met name in hoeverre aan deze bezwaren tegemoet is gekomen.

3. Het ontwerp situeert zich binnen de aanpak en afhandeling van onaanvaardbaar gedrag in en rond recreatiedomein. Overeenkomstig de toelichting bij het ontwerp beoogt de aanvrager te voorzien in een kader waarbij de uitbaters van recreatiedomeinen zelf een aantal veiligheidsvoorwaarden moeten creëren, zoals bijvoorbeeld het opstellen van een huishoudelijk regelement[3]. Vervolgens worden het toepassingsgebied *ratione temporis* (de uren waarbinnen het mogelijk is om administratieve sancties op te leggen) en *ratione materiae* (de sanctioneerbare overtredingen) vastgesteld. Concreet voor wat betreft de sancties die kunnen worden opgelegd, wordt gekeken naar de wet van 21 december 1998 *betreffende de veiligheid bij voetbalwedstrijden* (hierna: de voetbalwet), daar de aanvrager van oordeel is dat er belangrijke gelijkenissen bestaan tussen de geviseerde overtredingen in de beide regelgevingen.[4]

4. Daarnaast worden ook de modaliteiten vastgelegd voor het opleggen van officiële waarschuwingen en effectieve sancties, met inbegrip van de (bijzondere) regels inzake de kennisgeving van de beslissing, het aantekenen van beroep en de na te leven termijnen en uitzonderingen in dat verband.

---

[1] Te raadplegen via: https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-18-2023.pdf.

[2] Met name de vaststelling dat in het voormelde wetsvoorstel geen bepalingen werden opgenomen betreffende de voorwaarden waaronder en de omstandigheden waarin een persoon gesanctioneerd kon, gaven aanleiding tot een fundamentele opmerking over de rechtmatigheid van de geviseerde verwerkingen van persoonsgegevens. In het licht van de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie, en de artikelen 12 en 22 van de Grondwet, kan het voor de wetgever niet volstaan om inzake sanctionering louter te verwijzen naar de vrije wil van de uitbaters van recreatiedomeinen. Het is daarentegen de opdracht van de wetgever om, met inachtneming van de beginselen van voorspelbaarheid, noodzakelijkheid en evenredigheid, een wettelijk kader vast te stellen dat (1) bepaalt in welke omstandigheden en onder welke voorwaarden een persoon gesanctioneerd kan worden, en (2) een verplichting inhoudt voor de uitbaters van recreatiedomeinen tot (deelname aan de) handhaving en controle op de naleving van de opgelegde sancties. Zie in het bijzonder de punten 10 – 29 van het advies nr. 18/2023.

[3] Wat betreft de verplichting voor domeinuitbaters om een huishoudelijk regelement op te stellen, lijkt het aangewezen om uitdrukkelijk te preciseren dat daarin minstens de door het ontwerp geviseerde overtredingen opgenomen moeten worden. Bovendien lijkt het noodzakelijk om de voorwaarden vast te stellen waaronder de uitbater desgevallend verder kan gaan dan hetgeen wordt voorgeschreven door het ontwerp. In iedereen geval moeten de in het huiselijk regelement getroffen maatregelen te allen tijde aantoonbaar proportioneel zijn, en mogen zij niet van dien aard zijn dat bepaalde bevolkingsgroepen *ab initio* – direct of indirect – worden gediscrimineerd.

[4] Doch in dit verband wijst de Autoriteit op het negatieve advies n° 2024/3 van het FIRM betreffende het onderhavige wetsvoorstel, waarin het vermeende gerechtvaardigde karakter van de link met de voetbalwet sterk wordt betwist. Zie: https://federaalinstituutmensenrechten.be/sites/default/files/2024-12/20241128_Advies%20recreatiedomeinen%202024_NL.pdf.

5. Tot slot worden in Titel 7 van het ontwerp de regels inzake gegevensverwerking en informatie-uitwisseling vastgesteld. In deze context wordt de oprichting beoogd van een gecentraliseerd bestand van natuurlijke personen die het voorwerp hebben uitgemaakt van een of meerdere van de in het ontwerp bedoelde sancties. Dit bestand is toegankelijk voor de door de Koning aangewezen ambtenaren die belast zijn met het opleggen van deze sancties, alsook (beperkt) voor de uitbaters en de veiligheidsverantwoordelijken van recreatiedomeinen en de door hen aangeduide personen die betrokken zijn bij de toegangscontrole.

II. ONDERZOEK TEN GRONDE

a. Rechtsgrond

6. *Herhaling principes:* Elke norm die de verwerking van persoonsgegevens regelt (en die naar zijn aard een inmenging in het recht op bescherming van persoonsgegevens vormt) moet noodzakelijk en evenredig zijn en voldoen aan de vereisten van voorzienbaarheid en nauwkeurigheid in hoofde van de betrokkenen. Krachtens artikel 6.3 AVG, gelezen in samenhang met artikel 22 van de Grondwet en artikel 8 EVRM, moet een dergelijke wettelijke norm de essentiële elementen van de met de overheidsinmenging gepaard gaande verwerkingen vaststellen. Het gaat daarbij minstens om:
   - het (de) precieze en concrete doeleinde(n) van de gegevensverwerkingen;
   - de aanduiding van de verwerkingsverantwoordelijke(n) (tenzij dit duidelijk is).

   Wanneer de overheidsinmenging evenwel een belangrijke inmenging in de rechten en vrijheden van de betrokkenen vertegenwoordigt, dient de wettelijke norm tevens de volgende (aanvullende) essentiële elementen te omschrijven:
   - de (categorieën van) verwerkte persoonsgegevens die ter zake dienend en niet overmatig zijn;
   - de categorieën van betrokkenen wiens persoonsgegevens worden verwerkt;
   - de (categorieën van) bestemmelingen van de persoonsgegevens, evenals de omstandigheden waarin en de redenen waarom de gegevens worden verstrekt;
   - de maximale bewaartermijn van de geregistreerde persoonsgegevens.
   - de eventuele beperking van de verplichtingen en/of rechten vermeld in de artikelen 5, 12 tot 22 en 34 AVG.

7. *Toepassing van deze principe*s: In het onderhavige geval kan er, gelet op de aard en omvang van de geplande gegevensverwerkingen, de (categorieën van) betrokkenen, en de te verwerken (categorieën van) persoonsgegevens geen twijfel over bestaan dat er sprake is van een belangrijke inmenging in de rechten en vrijheden van betrokkenen. Het betreft immers verwerkingen die

plaatsvinden voor toezichts- of controledoeleinden, met name de bestraffing van personen, waaronder in voorkomend geval minderjarigen, die overtredingen in de zin van het ontwerp begaan. De identiteit van deze personen wordt samen met de overtreding(en) geregistreerd in een centraal bestand teneinde de sanctionerende ambtenaren en de uitbaters van recreatiedomeinen in staat te stellen de opgelegde sancties (waaronder bijvoorbeeld een domein- of perimeterverbod) te handhaven. Het is aldus noodzakelijk om ook de 'aanvullende' essentiële elementen van de verwerking vast te leggen in een formele wettelijke norm.

b. Doeleinde

8. Overeenkomstig artikel 5.1.b) AVG kan de verwerking van persoonsgegevens enkel uitgevoerd worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.

9. Hierboven werd reeds verduidelijkt dat het ontwerp gesitueerd is in de context van het sanctioneren van onaanvaardbaar gedrag in en rond recreatiedomeinen[5] en de effectieve handhaving van de opgelegde sancties.

10. In eerste instantie bepaalt artikel 33, §2, van het ontwerp: "*§ 1. De verwerking van gegevens bedoeld in paragraaf 1 geschiedt* ***met het oog op de sanctionering van eventuele inbreuken via een administratieve sanctie****."* Artikel 34, §§1 – 2, van het ontwerp specifieert vervolgens: "*Elke beslissing waarbij op grond van deze wet een waarschuwing, een administratieve geldboete of een administratief domeinverbod wordt opgelegd of waarbij een gerechtelijk domeinverbod of een domeinverbod als beveiligingsmaatregel wordt opgelegd, wordt meegedeeld aan een door de Koning aangewezen ambtenaar, volgens de nadere regels bepaald door de Koning door middel van een besluit vastgesteld na overleg in de Ministerraad.*
§2. De in paragraaf 1 bedoelde ***ambtenaar houdt één enkel bestand bij van de natuurlijke personen die het voorwerp hebben uitgemaakt van een of meerdere van de in paragraaf 1 bedoelde sancties.*** *(…)*
Dit bestand is bedoeld om ***het beheer van de sancties te verzekeren****."*
Paragraaf 5 van datzelfde artikel voegt daaraan toe: *"Voor de controle op de naleving van het opgelegde administratief of gerechtelijk domeinverbod of het domeinverbod als beveiligingsmaatregel, hebben de uitbater en de veiligheidsverantwoordelijke van een recreatiedomein toegang tot de persoonsgegevens in het register met het oog op het bekomen van een "hit/ no hit"-resultaat met betrekking tot de aan- of afwezigheid van een opgelegd domeinverbod. (…)*

[5] Artikel 2, 1°, van het ontwerp definieert recreatiedomein als: *"het door de Koning vastgestelde* ***omsloten*** *en voor het publiek toegankelijke domein met recreatieve voorzieningen dat wordt uitgebaat met het oog op de ontspanning van het publiek."* Deze definitie laat toe het feitelijke toepassingsgebied van het ontwerp af te bakenen, en komt aldus tegemoet aan één van de centrale kritieken geformuleerd in het bovengenoemde advies nr. 18/2023.

*Er is een **"hit"-resultaat** als een van de in het eerste lid bedoelde sancties werd opgelegd. In het geval van een "hit"-resultaat verkrijgt de raadpleger van het register de **bevestiging dat er een "hit"-resultaat is, samen met een afschrift van de opgelegde sanctie**.*
*Er is een **"no hit"-resultaat** als er geen in het eerste lid bedoelde sanctie werd opgelegd. In het geval van een "no hit"-resultaat, krijgt de raadpleger de **melding dat er een "no hit"-resultaat** is.*
De raadpleging gebeurt via een elektronische toegang waarvan de nadere regels door de Koning worden bepaald."

11. Het doeleinde van de verwerking is aldus tweeledig. In de eerste plaats dienen persoonsgegevens van (potentiële) overtreders te worden verwerkt teneinde overtredingen vast te kunnen stellen en om hen naderhand (al dan niet) te kunnen sanctioneren[6]. Vervolgens zullen deze gegevens worden geregistreerd, zodanig dat het voor de sanctionerende ambtenaren en domeinuitbaters mogelijk is om effectief toe te zien op de naleving van een domein- of perimeterverbod.

12. Hoewel de Autoriteit van oordeel is dat er in principe sprake is van welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden, meent zij niettemin dat – onverminderd de delegatie aan de Koning om de regels inzake de elektronische toegang tot het centraal sanctieregister voor de domeinuitbaters nader te bepalen – de modaliteiten van het 'hit/ no hit' systeem verder uitgewerkt, dan wel gepreciseerd moeten worden in het ontwerp, of minstens in de toelichting. De wijze van implementatie van de controle raakt immers wezenlijk aan het gerechtvaardigde karakter en de verhoopte proportionaliteit van de doeleinden. In de onderhavige context is het bijzonder belangrijk om daarbij de wijze van de controle te preciseren, en meer bepaald of het louter steekproefsgewijs[7] dan wel systematisch[8] zal gebeuren (het organisatorische aspect). Op technisch vlak vindt de controle plaats door middel van de voorlegging en uitlezing van de identiteitskaart van de betrokken bezoeker, teneinde na te gaan of hij voorkomt in het centraal register, en meer bepaald of er aan deze persoon een domein- of perimeterverbod werd opgelegd.

13. Zoals uitvoerig werd toegelicht in advies nr. 18/2023 kan het daartoe volstaan dat de door de Koning aangewezen ambtenaar het sanctieregister ter beschikking stelt in de vorm van een lijst bestaande uit de gehashte identificatiegegevens van de betrokkenen, versterkt met een 'Cuckoo Filter' (of koekoeksfilter). Een koekoeksfilter bestaat uit een filterbestand dat geregeld (bijvoorbeeld op dagelijkse of wekelijkse basis) wordt aangemaakt op basis van de gehashte

[6] Artikel 23 van het ontwerp voorziet immers in een verjaringstermijn van zes maanden voor opleggen van een administratieve sanctie, te rekenen van de dag waarop het feit werd gepleegd, de mogelijke beroepsprocedures niet inbegrepen.

[7] In dit geval bestaat er uiteraard een belangrijk risico op discriminatie ten aanzien van bepaalde groepen die systematisch – terecht, dan wel onterecht – in verband worden gebracht met problematisch gedrag in en rond recreatiedomeinen.

[8] Aangezien het ontwerp een recreatiedomein omschrijft als een omsloten, doch voor het publiek toegankelijk domein, is het in deze mogelijk om te opteren voor een systematische identiteitscontrole aan de ingang.

identiteitsgegevens van alle personen aan wie een sanctie werd opgelegd op grond waarvan aan hen de toegang tot het recreatiedomein kan worden ontzegd. Bij de toegangscontrole wordt de identiteitskaart van de betrokkene via een programma gekruist of vergeleken met het filterbestand, wat resulteert in een 'hit' of 'no-hit' resultaat. De filter kan bijkomend verfijnd worden, indien het wenselijk zou zijn om naast het bestaan van een actieve sanctie ook de aard van de sanctie[9] en de maand of week waarin de sanctie afloopt weer te geven. Rekening houdend met het feit dat de eID van de betrokkene hoe dan ook voorgelegd moet worden tijdens de toegangscontrole, is de Autoriteit van oordeel dat de vermelding van de aard van de sanctie (en desgevallend de periode waarin deze afloopt) in het geval van een 'hit' resultaat kan volstaan teneinde de legitimiteit van een toegangsweigering door de controleur te verifiëren, doch ook te motiveren naar de geweigerde bezoeker toe.

14. Voorts merkt de Autoriteit op dat er tijdens de toegangscontrole geen logging mag plaatsvinden op de apparatuur die de identiteitskaart uitleest en de informatie doorstuurt naar het programma.

15. De hierboven geschetste manier van werken laat toe te verhinderen dat dienst die het centraal sanctiebestand bijhoudt informatie zou ontvangen over de identiteit van de bezoekers van een recreatiedomein, aangezien de verificatieprocedure geheel lokaal en offline gebeurt (er vindt met andere worden geen koppeling plaats tussen de resultaten van de toegangscontrole en het centraal bestand). Bovendien wordt er vermeden dat de domeinuitbater (of diens aangestelden) rechtstreeks toegang zouden hebben tot de persoonsgegevens in het bestand (het is immers enkel mogelijk om met behulp van het programma na te gaan of een specifieke bezoeker (waarvan de gegevens gekend zijn) al dan niet voorkomt op de lijst). Teneinde een zeker vorm van *ex post* controle mogelijk te maken[10] is het wel aanvaardbaar dat het programma aan de dienst (de verwerkingsverantwoordelijke van het bestand) zou rapporteren hoeveel keer het gebruikt werd (per dag of per week) en hoeveel 'hits' er zijn geweest.

16. In dat verband nog verdient het aanbeveling om de procedure te preciseren die moet worden gevolgd wanneer aan de ingang van een recreatiedomein wordt vastgesteld dat de bezoeker een eID voorlegt die overduidelijk niet aan hem toebehoort, of überhaupt niet over een Belgische identiteitskaart beschikt (bijvoorbeeld toeristen). Ook moet er bijzondere aandacht worden besteed aan de bescherming van de inloggegevens van gebruikers, bijvoorbeeld wanneer een toegangsticket online aangekocht kan worden en er op dat ogenblik reeds een verificatie zou plaatsvinden (via een eID-kaartlezer of itsme). Ten slotte moet het ontwerp voorzien in een mogelijkheid tot nazicht in geval van een vermoedelijk foutieve registratie in het centraal

[9] In dit geval kan het evenwel enkel gaan over een administratief of gerechtelijk domeinverbod, of een domeinverbod opgelegd als beveiligingsmaatregel. Het bestaan van een boete vormt immers geen geldige uitsluitingsgrond.

[10] Bijvoorbeeld om misbruik (of niet-gebruik) van het systeem te detecteren.

sanctiebestand[11] (hetgeen aanleiding zou geven tot een onterechte toegangsweigering). Het bestaan van een dergelijke mogelijkheid en de modaliteiten ervan moeten opgenomen worden in het huishoudelijk regelement, en moeten raadpleegbaar zijn op elke plaats waar een identiteitscontrole kan plaatsvinden.

17. Ten algemene titel merkt de Autoriteit nog op dat een eventuele systematische identiteitscontrole een inmenging zou vormen in de grondrechten van alle personen die toegang krijgen of wensen te krijgen tot een recreatiedomein, waarbij er dus ten alle tijde gewaakt moet worden over het evenwicht tussen het belang om de openbare rust en orde in recreatiedomeinen te handhaven/ verzekeren enerzijds, en de grondrechten van de betrokkenen inzake privacy en gegevensbescherming anderzijds. Indien er daarentegen sprake is van selectieve of steekproefsgewijze controles, moet er bijzondere aandacht worden besteed aan het verhoogde risico op discriminatie. Daartoe is het noodzakelijk om minstens intern (desgevallend via de interne richtlijnen van elk recreatiedomein) afspraken te maken, teneinde ervoor te zorgen dat er een objectief onderbouwde grondslag bestaat voor de toegangscontrole, en dat het gerandomiseerde of willekeurige karakter ervan vaststaat en aantoonbaar is.

c. Verwerkingsverantwoordelijke

18. Overeenkomstig artikel 4.7) AVG is de verwerkingsverantwoordelijke elke natuurlijke of rechtspersoon, overheidsinstantie, dienst of ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen. Volledigheidshalve brengt de Autoriteit in herinnering dat de aanduiding van de verwerkingsverantwoordelijke passend moet zijn in het licht van de feitelijke omstandigheden. Zowel het Europees Comité voor gegevensbescherming als de Autoriteit hebben aangedrongen op de noodzaak om deze concepten te benaderen vanuit een feitelijk perspectief. Het is derhalve noodzakelijk de entiteit of entiteiten aan te wijzen die in feite het doel van de verwerking nastreven en de controle erover uitoefenen.

19. Daarnaast merkt de Autoriteit op dat wanneer er sprake is van een gezamenlijke verantwoordelijkheid voor de verwerking, artikel 26 AVG van toepassing is, en verwijst voor de praktische gevolgen daarvan naar punt 2 van het tweede deel van de op 2 september 2020 door de Europese Comité voor gegevensbescherming vastgestelde richtsnoeren 07/2020 betreffende

[11] De Autoriteit benadrukt dat het hier niet gaat over een bijkomende beroepsprocedure jegens opgelegde en in kracht van gewijsde getreden sancties.

de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG[12]. Met name zal op transparante wijze moeten worden bepaald wie verantwoordelijk is om de betrokkenen die hun rechten in het kader van de AVG uitoefenen te beantwoorden (onverminderd het feit dat, overeenkomstig artikel 26.3 van de AVG, de betrokkenen hun rechten in het kader van de AVG kunnen uitoefenen ten aanzien van elk van de gezamenlijke verwerkingsverantwoordelijken).

20. In eerste instantie voorziet artikel 33, §3, van het ontwerp: *"Voor de verwerking van deze persoonsgegevens is de dienst van de ambtenaar bedoeld in artikel 16, §1, eerste lid bevoegd."* Het betreft met name de gegevens die door de door de Koning aangewezen ambtenaar worden verwerkt met het oog op de sanctionering van eventuele inbreuken via een administratieve sanctie (de sanctionerende ambtenaar). Uit de toelichting volgt dat deze dienst, naar analogie met de Voetbalwet, de FOD Binnenlandse zaken zal zijn. Mogelijks zal het de huidige voetbalcel zijn die feitelijk wordt belast met deze opdracht.

21. Artikel 34, §2, van het ontwerp bepaalt vervolgens: *"De in paragraaf 1 bedoelde ambtenaar houdt één enkel bestand bij van de natuurlijke personen die het voorwerp hebben uitgemaakt van een of meerdere van de in paragraaf 1 bedoelde sancties. De dienst waarvoor de ambtenaar werkt, is verantwoordelijk voor de verwerking van dit bestand."*

22. Ter zake is de Autoriteit van oordeel dat voor wat betreft de vaststelling en sanctionering van overtredingen, alsook de registratie van overtredingen in het centraal sanctieregister, de aanduiding van de dienst (FOD Binnenlandse Zaken) als verwerkingsverantwoordelijke overeenstemt met de rol die deze actor in de praktijk zal opnemen. Desalniettemin verdient het aanbeveling om in deze ook reeds de concrete hoedanigheid van de domeinuitbaters vast te stellen. Uit hoofde van het ontwerp worden aan de domeinuitbaters immers bepaalde verplichtingen en bevoegdheden opgelegd/ toegewezen. De uitbaters (of diens aangestelden) moeten een huishoudelijk regelement opstellen[13] en toezien op de naleving van opgelegde domeinverboden, in het kader waarvan zij bepaalde gegevens van hun bezoekers dienen te verwerken en, bovendien, (indirect en beperkt) toegang kunnen nemen tot het sanctieregister overeenkomstig artikel 34, §5, van het ontwerp. Voor deze verwerkingsdoeleinden moet aldus worden nagegaan of er sprake is van enkelvoudige of gezamenlijke verantwoordelijkheid, dan wel van een verwerkersrelatie in de zin van artikel 28 AVG[14]. Afhankelijk van de concrete kwalificatie zullen de respectieve bepalingen van de AVG in acht moeten worden genomen.

---

[12] Te raadplegen via de volgende link (let op: deze vertaling werd nog niet officieel goedgekeurd): https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_nl.pdf.

[13] Zie ook *supra* voetnoot 3.

[14] Dit heeft uiteraard geen invloed op de verantwoordelijkheid die de domeinuitbaters dragen voor de gegevensverwerkingen die desgevallend plaatsvinden in het kader van het normale beheer en de exploitatie van recreatiedomeinen (logistiek, HR…).

23. In deze context dient ook opgemerkt te worden dat de bepalingen van het ontwerp, en meer bepaald de aanduiding van de FOD Binnenlandse Zaken als verwerkingsverantwoordelijke voor de sanctionering van eventuele inbreuken en het beheer van het sanctieregister geen afbreuk doet aan de verantwoordelijkheid van de (externe) bewakingsagenten, de (lokale) politiediensten (de verbalisanten) en, in voorkomend geval, het openbaar ministerie voor de gegevensverwerkingen die zij uitvoeren in de context van hun wettelijke opdrachten.

24. Tot slot (eerder redactioneel), rekening houdend met de vaststelling dat de term 'verwerkingsverantwoordelijke' verscheidene keren wordt gebruikt doorheen het ontwerp, beveelt de Autoriteit aan om in artikel 33, §3, van het ontwerp de betrokken dienst (met name FOD Binnenlandse Zaken) uitdrukkelijk aan te duiden als de verwerkingsverantwoordelijke[15]. Op heden wordt er immers louter gesteld dat de voormelde dienst bevoegd is voor de geviseerde gegevensverwerkingen. Zulks geeft aanleiding tot interpretatieproblemen, in het bijzonder bij de lezing van artikel 34 van het ontwerp, uit hoofde waarvan de domeinuitbaters bepaalde gegevens moeten meedelen aan 'de verwerkingsverantwoordelijke'. In deze context is aldus cruciaal dat de identiteit van de verwerkingsverantwoordelijke ondubbelzinnig vaststaat.

d. Proportionaliteit/ Minimale gegevensverwerking

25. Artikel 5.1.c), AVG bepaalt dat persoonsgegevens toereikend, terzake dienend en beperkt moeten zijn tot wat noodzakelijk is voor de beoogde doeleinden (principe van 'minimale gegevensverwerking').

26. Ter zake dient een onderscheid te worden gemaakt tussen de verwerking van persoonsgegevens van bezoekers en (potentiële) overtreders enerzijds (zowel inzake de sanctionering *an sich,* als de vermelding in het centraal sanctiebestand), en de verwerking van de persoonsgegevens van bepaalde medewerkers van de domeinuitbaters anderzijds.

27. In eerste instantie voorziet artikel 33, §1, eerste lid, van het ontwerp, dat betrekking heeft op de verwerkingen die geschieden met het oog op de sanctionering van eventuele inbreuken: *"In het kader van de toepassing van deze wet kunnen de volgende persoonsgegevens worden verwerkt: de identificatiegegevens van de overtreder, meer bepaald zijn naam, voornamen, en geboortedatum, hoofdverblijfplaats, rijksregisternummer, de gegevens betreffende de bekwaamheid en de vertegenwoordiging en de gegevens betreffende de voogdij en de afstamming."*

[15] In dat verband moet opgemerkt worden dat de toelichting bij artikel 33 van het ontwerp stelt dat de sanctionerende ambtenaar optreedt als verwerkingsverantwoordelijke. Dit is in strijd met de tekst van artikel 33 van het ontwerp, en strookt bovendien niet met de geest van de toelichting bij artikel 16 van het ontwerp. De betrokken passage dient nuttig gewijzigd te worden.

28. Ten aanzien van de naam, voornamen, geboortedatum en hoofdverblijfplaats formuleert de Autoriteit geen bijzondere opmerkingen.

29. Wat de verwerking van rijksregisternummer betreft onderschrijft de Autoriteit het belang van correcte identificatie en het daarbij verwerken van gegevens die voldoen aan de vereisten van kwaliteit en juistheid. Ze wijst er evenwel op dat het gebruik van het Rijksregisternummer in België strikt geregeld wordt door artikel 8 van de wet van 8 augustus 1983 *tot regeling van een Rijksregister van de natuurlijke personen*. De Autoriteit herinnert er ook in het algemeen aan dat unieke identificatienummers een bijzondere bescherming genieten. Artikel 87 AVG voorziet dat de lidstaten die een nationaal identificatienummer vaststellen, er moeten over waken dat dit alleen wordt gebruikt met passende waarborgen voor de rechten en vrijheden van de betrokkene. Zo vestigde de Commissie voor de bescherming van de persoonlijke levenssfeer, de rechtsvoorganger van de Autoriteit, reeds eerder[16] de aandacht op de in acht te nemen waarborgen ter zake:
    - het gebruik van een algemeen identificatienummer moet worden beperkt tot de gevallen waarin dit strikt noodzakelijk is aangezien dit gebruik risico's impliceert inzake koppeling van bestanden;
    - de doeleinden moeten duidelijk en expliciet worden gepreciseerd zodat men de beoogde soorten verwerkingen kan vermoeden/voorzien;
    - de bewaartermijn en de eventuele mededelingen aan derden moeten eveneens worden omkaderd;
    - technische en organisatorische maatregelen moeten het beveiligd gebruik passend omkaderen en
    - de niet-naleving van de bepalingen die het gebruik omkaderen moeten worden gesanctioneerd aan de hand van effectieve, proportionele en ontradende sancties.

30. Ter zake vraagt de Autoriteit zich af of het niet aangewezen is om tevens melding te maken van het *bis*-nummer, daar niet elke overtreder noodzakelijkerwijze over een rijksregisternummer zal beschikken.

31. Daarnaast meent de Autoriteit dat het noodzakelijk is om bijkomend te verduidelijken waarop de notie 'bekwaamheid' concreet betrekking heeft, en met welk oogmerk dit informatiegegeven verwerkt zal worden. Bekwaamheid kan immers gelieerd worden aan de leeftijd (jonger dan veertien jaar, tussen veertien en achttien jaar of meerderjarig), doch ook aan de (niet-leeftijdsgebonden) handelsbekwaamheid van de betrokkene. Dit onderscheid is belangrijk daar indien uitsluitend de laatste categorie wordt beoogd, er in voorkomend geval sprake zal zijn van

[16] Zie advies nr. 19/2018 van 29 februari 2018 betreffende een voorontwerp van wet *houdende diverse bepalingen "Binnenlandse Zaken"*.

een verwerking van gezondheidsgerelateerde of anderszins gevoelige persoonsgegevens, die een bijzondere bescherming genieten op grond van artikel 9.1 AVG, en waarvan de verwerking slechts mogelijk is indien er beroep kan worden gedaan op een van de uitzonderingsgronden vermeld in artikel 9.2 AVG. In de onderhavige context kan de verwerking van dergelijke gegevens slechts gerechtvaardigd worden wanneer zulks absoluut en aantoonbaar noodzakelijk is om een bepaalde situatie *in concreto* te beoordelen[17]. Bijvoorbeeld wanneer de handelsonbekwaamheid van de betrokkene tot gevolg zou hebben dat er geen sprake is van een overtreding in de zin van het ontwerp, of wanneer dit aanleiding zou geven tot verzachtende omstandigheden. In ieder geval verzoekt de Autoriteit om de notie 'leeftijd' en 'bekwaamheid' afzonderlijk op te nemen in het ontwerp, en om – bijvoorbeeld in de toelichting – uitdrukkelijk te preciseren op welke manier het begrip 'bekwaamheid' moet worden geïnterpreteerd.

32. Wat tot slot '*de gegevens betreffende de voogdij en de afstamming'* betreft, acht de Autoriteit het noodzakelijk om in de toelichting te preciseren dat 'afstamming' in deze context louter betrekking heeft op de vaststelling van het ouderschap en om, naar analogie met artikel 34, §3, eerste lid, van het ontwerp[18], de volgende zinsnede toe te voegen: "*… **in het geval van een minderjarige**, de gegevens betreffende de voogdij en de afstamming.*"

33. Artikel 34, §3, eerste lid, van het ontwerp bepaalt vervolgens welke gegevens in het centraal sanctiebestand opgenomen worden: "*§3. Dit bestand bevat de volgende persoonsgegevens en informatiegegevens:*
    1° *de naam, de voornamen, geboortedatum en hoofdverblijfplaats van de personen die het voorwerp uitmaken van sancties; in het geval van een minderjarige, de namen, voornamen, geboortedatum en de hoofdverblijfplaats van iedere titularis die het ouderlijk gezag heeft over de minderjarige;*
    2° *de aard van de gepleegde feiten;*
    3° *de aard van de sanctie en de dag waarop deze werd opgelegd;*
    4° *de sancties waartegen geen beroep meer ingesteld kan worden."*

34. Hoewel de bovenstaande gegevenscategorieën in het licht van hetgeen hierboven reeds werd uiteengezet geen bijzondere (bijkomende) opmerkingen noodzaken, meent de Autoriteit dat het met het oog op de *ex post* controle op de naleving van domein- of perimeterverboden niettemin noodzakelijk is om ook het rijksregisternummer of *bis*-nummer van de overtreder te registreren in het bestand. In de mate immers dat deze controle plaatsvindt door de voorlegging en uitlezing van de identiteitskaart van de betrokkene, is het rijksregister- of *bis*-nummer het gegeven bij

[17] Dit wil zeggen dat dergelijke gegevens slechts in secundaire orde verwerkt kunnen worden, wanneer uit een concrete situatie kan worden afgeleid dat de handels(on)bekwaamheid van (een van) de betrokkenen een wezenlijk element vormt bij de beoordeling van de ernst van de feiten of bij het bepalen van de strafmaat.

[18] Zie ook infra punt 33 e.v.

uitstek om na kruising met het centraal bestand een '*hit/ no hit'* resultaat te bekomen. Het ontwerp dient nuttig gewijzigd te worden in voormelde zin. Daarnaast lijkt het aangewezen om te preciseren dat ook de foto van de betrokkene (op de identiteitskaart) verwerkt kan worden, in het bijzonder met het oog op de toegangscontrole (teneinde in eerste instantie te kunnen vaststellen dat de persoon op de foto dezelfde is als diegene die zijn eID voor controle aanbiedt).

35. In tweede instantie worden ook de identificatiegegevens van bepaalde medewerkers van de domeinuitbaters verwerkt. In dat verband bepaalt artikel 34, §5, van het ontwerp: "§5. *De uitbater en de veiligheidsverantwoordelijke van een recreatiedomein kunnen hun toegang tot het register delegeren aan het schriftelijk bij naam aangewezen personen die betrokken zijn bij de toegangscontrole. Deze delegatie moet met redenen omkleed zijn en verantwoord zijn door de noodwendigheden van de dienst. De lijst van deze bij naam aangewezen personen dient door de uitbater en de veiligheidsverantwoordelijke onverwijld te worden meegedeeld aan de verwerkingsverantwoordelijke. De lijst van personen die alzo toegang hebben tot het register wordt door de verwerkingsverantwoordelijke ter beschikking gehouden van de Gegevensbeschermingsautoriteit. De verwerkingsverantwoordelijke zorgt ervoor dat de aangewezen personen ertoe gehouden zijn het vertrouwelijke karakter van de betrokken gegevens in acht te nemen."*

36. Ter zake lijkt het met het oog op logging en het toezicht op de identiteitscontrole verantwoordbaar dat er een lijst wordt bijgehouden van de personen die instaan voor de toegangscontrole en dat deze lijst ter beschikking wordt gehouden van de Autoriteit. Zulks doet evenwel geen afbreuk aan hetgeen uiteengezet in punt 13, namelijk dat de 'toegang' tot het centraal sanctieregister voor de domeinuitbaters of diens aangestelden beperkt moet blijven tot gehashte gegevens van de betrokkenen, waarbij na uitlezing van de eID louter een 'hit' resultaat met vermelding van de aard van de sanctie of een 'no-hit' resultaat wordt weergegeven.

37. Tot slot – in de mate dat **de perimeter** rond het recreatiedomein **een gebied impliceert waarbinnen persoonsgegevens van eenieder zouden kunnen worden verwerkt ter vrijwaring van de in het ontwerp vermelde doeleinden** – spreekt de Autoriteit haar meer algemene bezorgdheid uit over de legitimiteit en het gerechtvaardigde karakter van de mogelijkheid om binnen de context van het ontwerp sancties op te leggen in deze perimeter, dewelke maximaal wordt vastgesteld op **een straal van 1.000 meter** vanaf de omsluiting van het recreatiedomein. Ter zake is de Autoriteit van oordeel dat een dergelijke ruime straal onvoldoende (lees: niet) wordt gerechtvaardigd en aldus in verschillende opzichten vragen doet rijzen over de proportionaliteit van dergelijke maatregelen. Zulks geldt in het bijzonder rekening houdend met het arrest nr. 44/2015 van het Grondwettelijk Hof, waarin het Hof – inzake het

plaatsverbod[19] – heeft geoordeeld dat dit alleen verenigbaar is met de persoonlijke bewegingsvrijheid voor zover de perimeter in kwestie niet ruimer is dan hetgeen noodzakelijk is om de verstoring van de openbare orde verhinderen of te beëindigen. Een perimeterverbod dat tot 1.000 meter voorbij de buitengrenzen van het recreatiedomein kan omvatten, gaat veel verder dan noodzakelijk is voor de doelstelling om te "*vermijden dat onlusten zich verplaatsen buiten de grenzen van het recreatiedomein*" – een doelstelling die trouwens evengoed nagestreefd kan worden via een beroep op de normale politiebevoegdheden waarover burgemeesters beschikken krachtens de Nieuwe Gemeentewet.[20]

38. Vooreerst kan er menens de Autoriteit in deze geen vergelijk plaatsvinden tussen de voetbalwet enerzijds, en de beveiliging van recreatiedomeinen anderzijds. Perimeter-gerelateerde maatregelen in de voetbalwet streven er (in eerste instantie) immers toe ((tien)duizenden) supporters en ordehandhavingsdiensten te beschermen die zich voor of na een voetbalwedstrijd in de nabijheid van een stadium bevinden, of om georganiseerde bussen met hooligans tijdig te onderscheppen om de identiteit van de inzittenden vast te kunnen stellen. Het perimeterverbod in de voetbalwet is bovendien veel beperkter in tijd: het geldt vanaf vijf uur voor aanvang van de voetbalwedstrijd tot vijf uur na afloop hiervan[21]. Deze doeleinden kunnen aldus niet *mutatis mutandis* worden aangevoerd als rechtvaardigingsgrond in de onderhavige context. Het spreekt voor zich dat ook de eenvoudige vermelding in de toelichting bij artikel 2 van het ontwerp dat "*de incidenten die we de laatste jaren hebben gekend rond recreatiedomeinen zich ook buiten de omsluiting van deze domeinen hebben afgespeeld*" bezwaarlijk de verregaande aard van bepaalde maatregelen kan verantwoorden.

39. In tweede instantie – opnieuw rekening houdend met de bijzonder ruim vastgestelde perimeter – vraagt de Autoriteit zich af op welke wijze de verbaliserende ambtenaar het verband moet aantonen tussen de overtredingen bedoeld in de artikelen 6 (gooien van voorwerpen) en 11 (aanzetten tot haat of geweld) van het ontwerp en de vrijwaring van de veiligheid in recreatiedomeinen. Dergelijke overtredingen kunnen immers nu reeds gesanctioneerd worden, zonder dat het daartoe vereist is dat de overtreder in kwestie handelt met het oogmerk amok te maken in of rond het recreatiedomein. In de mate dat naar aanleiding van dergelijke feiten er een domein- of perimeterverbod zou worden opgelegd, moet het verband met (de beveiliging van) het recreatiedomein ondubbelzinnig vaststaan en aantoonbaar zijn.

40. Ten derde wijst de Autoriteit op de strikte voorwaarden die krachtens hoofdstuk 3 van de wet van 2 oktober 2017 *tot regeling van de private en bijzondere veiligheid* van toepassing zijn op interne

[19] Artikel 134*sexies*, Nieuwe Gemeentewet.

[20] Zie bijvoorbeeld artikel 133, eerste lid en artikel 135, §2, Nieuwe Gemeentewet.

[21] Artikel 24, §1, derde lid, Voetbalwet.

bewakingsdiensten. In dat verband herinnert de Autoriteit eraan dat de bewakingsagenten van dergelijke (**vergunde**) diensten overeenkomstig artikel 24, vierde lid, j° artikel 115, 2°, van dezelfde wet op de openbare weg (lees: de perimeter van het recreatiedomein) enkel bewakingsactiviteiten kunnen uitoefenen die betrekking hebben op evenementenbewaking. Zulks valt moeilijk te rijmen met artikel 8 van het ontwerp dat bepaalt: *"(…) kan eenieder die in het recreatiedomein of **in de perimeter** de richtlijnen of bevelen van een bewakingsagent of **een lid van de interne bewakingsdienst** in de uitvoering van hun functie (…), niet opvolgt, één of meerdere sancties oplopen zoals bedoeld in de artikelen 12 en 13."* Een dergelijke bevoegdheid zou immers (minstens) vereisen dat de betrokken bewakingsagent (van de interne dienst) in staat is om personen identiteitsdocumenten te laten voorleggen (buiten de context van de toegangscontrole) of om ze te vatten en in afwachting van de politiediensten, te verhinderen dat ze weglopen. Het spreekt aldus voor zich dat artikel 8 van het ontwerp grondig gewijzigd dient te worden in overeenstemming met de voorschriften van de voormelde wet.

41. Samenvattend meent de Autoriteit dat het zonder meer noodzakelijk is om zowel de omvang van de perimeter als de aard en de ernst van mogelijke sancties in dat verband grondig te herzien en uitdrukkelijk te motiveren in de toelichting. Op heden ziet de Autoriteit zich immers genoodzaakt om resoluut negatief te adviseren over dit aspect van het ontwerp.

e. Bewaartermijn

42. Krachtens artikel 5.1.e) AVG mogen persoonsgegevens niet langer worden bewaard, in een vorm die het mogelijk maakt de betrokkenen te identificeren, dan noodzakelijk voor de verwezenlijking van de doeleinden waarvoor zij worden verwerkt.

43. In eerste instantie voorziet artikel 33, §4, van het ontwerp: "*De persoonsgegevens worden bewaard gedurende een periode die maximaal gelijk is aan de bewaartermijn van de gegevens in het register overeenkomstig artikel 34.*[22] *De persoonsgegevens worden maximaal bewaard gedurende de periode waarin een administratieve sanctie kan worden opgelegd overeenkomstig artikel 23*[23]*. Indien effectief wordt overgegaan tot het opleggen van een administratieve sanctie, gelden de bewaartermijnen van artikel 34. De persoonsgegevens worden in ieder geval niet langer bewaard dan nodig is voor de doeleinden waarvoor ze worden verwerkt.*[24]*"*

[22] Aan deze zin ontbreekt een punt in het ontwerp.

[23] Artikel 23 regelt de verjaringstermijn voor de (sanctionering van) administratieve inbreuken. De administratieve vordering verjaart na verloop van zes maanden, te rekenen van de dag waarop de inbreuk heeft plaatsgevonden. Zulks impliceert dat wanneer geen sanctie werd opgelegd binnen de zes maanden na het plegen van de feiten, alle in dat verband verzamelde persoonsgegevens onverwijld vernietigd (dan wel geanonimiseerd) moeten worden.

[24] Louter redactioneel meent de Autoriteit dat de volgende wijzigingen aan de voormelde paragraaf zich opdringen:

- schrappen van de eerste zin, deze biedt immers geen juridische meerwaarde ten aanzien van het vervolg van de paragraaf;

44. Artikel 34, §3, tweede lid, van het ontwerp bepaalt op zijn beurt: *"De in het eerste lid bedoelde gegevens worden gedurende vijf jaar bewaard, te rekenen van de datum waarop de sanctie werd opgelegd. Wanneer deze termijn verstreken is, worden zij hetzij vernietigd, hetzij geanonimiseerd."*

45. De Autoriteit is van oordeel dat een dergelijke termijn te rechtvaardigen valt in het licht van de maximale duur van een domein- of perimeterverbod (te weten vijf jaar) en de op heden geldende bewaartermijn voor gemeentelijke administratieve sancties. Desalniettemin lijkt het in dat geval aangewezen om de bewaartermijn te laten lopen vanaf het moment dat de sanctie in kracht van gewijsde treedt (na het verstrijken van de beroepstermijn, of na uitputting van alle rechtsmiddelen), teneinde geen verwarringen te laten bestaan over wanneer de sanctie werd opgelegd.

46. Een dergelijke bewaartermijn doet evenwel geen afbreuk aan het feit dat het voor de domeinuitbater of diens aangestelden na afloop van een domeinverbod geenszins mogelijk kan zijn om kennis te nemen van het bestaan van dat domeinverbod.[25]

47. Voor de gegevens die worden verwerkt door politie en justitie kan uiteraard verwezen worden naar de voor hen geldende bewaartermijnen overeenkomstig hun respectieve kaderwetgeving.

48. In tweede instantie stelt de Autoriteit vast dat er geen bewaartermijn wordt vastgesteld voor de identificatiegegevens van de bij de toegangscontrole betrokken personen. Het is noodzakelijk om ook voor deze gegevens een maximale bewaartermijn vast te stellen. Deze bewaartermijn kan in geen geval langer zijn dan de bewaartermijnen die worden vastgesteld voor de loggegevens (*infra*).

49. Tot slot nog formuleert de Autoriteit een aantal opmerkingen met betrekking tot de bewaartermijnen die worden vastgesteld voor de loggegevens overeenkomstig respectievelijk de artikelen 33, §5 en 34, §6, van het ontwerp:
    - aangezien de in artikel 33 van het ontwerp vermelde gegevensverwerkingen in eerste instantie betrekking hebben op de feitelijke vaststelling en sanctionering van overtredingen, vraagt de Autoriteit zich af welke raadplegingen het voorwerp uit dienen te maken van de

---

- in de tweede zin, naar analogie met de toelichting bij het ontwerp, toevoegen: "*In de gevallen waarin er geen administratieve sanctie wordt opgelegd, worden de persoonsgegevens maximaal bewaard (…) overeenkomstig artikel 23.*";
- schrappen van de vierde en laatste zin, deze betreft immers een schending van het overschrijfverbod van de AVG, en heeft bovendien geen enkele meerwaarde ten aanzien van artikel 5.1.e) AVG.

[25] Wanneer een bezoeker na afloop van het aan hem opgelegd domeinverbod opnieuw toegang wenst te verkrijgen tot een recreatiepark, mag er enkel sprake zijn van een '*no hit*' resultaat bij de toegangscontrole, zonder meer.

voorgeschreven logging[26]. Het verdient aanbeveling om dit nader te preciseren. De Autoriteit vraagt zich tevens af welke rechtvaardigingsgrond er bestaat voor de bewaartermijn van vijf jaar, te rekenen van de afloop van de bewaartermijn vermeld in artikel 33, §4, van het ontwerp. De afloop van deze laatste termijn impliceert immers dat er geen sanctie werd opgelegd, dan wel dat de straf in kwestie werd uitgevoerd, dat er geen enkel rechtsmiddel meer tegen openstaat en dat de betrokken persoonsgegevens werden vernietigd of geanonimiseerd. Als dusdanig ziet de Autoriteit niet in welke meerwaarde deze bijkomende bewaartermijn voor de loggegevens biedt, en verzoekt ze om deze passend in te korten[27];

- wat de bewaartermijn van de in artikel 34, eerste lid, 2°, van het ontwerp bedoelde logbestanden betreft[28], is de Autoriteit hoe dan ook van oordeel dat een verduidelijking aan de orde is. Op heden wordt immers de indruk gewekt dat de logbestanden *ad infinitum* zullen worden bewaard zolang het centraal sanctiebestand wordt bijgehouden, hetgeen de noodzakelijkheids- en proportionaliteitstoets bezwaarlijk kan doorstaan. Naar analogie met hetgeen in het vorige streepje werd beargumenteerd, is de Autoriteit van oordeel dat een bewaartermijn (voor de logbestanden) van hoogstens twee jaar na de definitieve schrapping van een dossier uit het centraal bestand ruimschoots kan volstaan.

OM DEZE REDENEN,
de Autoriteit,

is van oordeel dat de volgende wijzingen aan het ontwerp zich opdringen:

- nader uitwerken van de modaliteiten van het '*hit/no hit*' systeem overeenkomstig hetgeen uiteengezet in de punten 12 – 17;
- vaststellen van de hoedanigheid van de domeinuitbater in het kader van de toegangscontrole en de 'raadpleging' van het centraal sanctiebestand (punt 22);
- expliciet aanduiden van de dienst als verwerkingsverantwoordelijke (punt 24);
- naast het rijksregisternummer ook het *bis*-nummer vermelden (punt 30);
- verduidelijken van de notie 'bekwaamheid' (punt 31);
- preciseren dat de notie 'afstamming' louter betrekking heeft op de vaststelling van het ouderschap (punt 32);

[26] Behoudens vergissing is er op dit ogenblik immers nog geen sprake van een registratie in het centraal bestand, hetgeen de vraag doet rijzen waarop de logbestanden betrekking (moeten) hebben.

[27] Een bijkomende bewaartermijn voor de logbestanden van 2 jaar na afloop van de oorspronkelijke bewaartermijn lijkt in dit geval ruimschoots te kunnen volstaan.

[28] Artikel 34, §6, derde lid, van het ontwerp voorziet: "*De bewaartermijn van de in het eerste lid, 2°, bedoelde logbestanden is maximaal vijf jaar, te rekenen van de laatst uitgevoerde handeling in het register. (…)*"

- rijksregister- en *bis*-nummer, evenals de foto van de betrokkene bijkomend opnemen in de te verwerken categorieën van persoonsgegevens (punt 34);
- herzien van de omvang van de perimeter, alsook van de aard en de ernst van de sancties die in de perimeter kunnen worden opgelegd in het licht van hetgeen uiteengezet in de punten 37 – 41;
- preciseren dat de bewaartermijn voor de persoonsgegevens begint te lopen vanaf het moment dat de sanctie kracht van gewijsde verkrijgt (punt 45);
- vaststellen van een (maximale) bewaartermijn voor de lijst van de bij de toegangscontrole betrokken personen 48;
- de bepalingen inzake de bewaartermijnen voor de logbestanden herzien overeenkomstig hetgeen uiteengezet in punt 49.

Voor de Autorisatie- en Adviesdienst,
Cédrine Morlière, Directeur

Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 06/2025 du 30 janvier 2025

Objet : Avis concernant une proposition de loi relative à la sécurité dans les domaines récréatifs (les articles 14, 16, 20, 21, 25, 32, 33, 34) (CO-A-2024-282)

Traduction

Introduction

La proposition de loi *relative à la sécurité dans les domaines récréatifs* qui est soumise pour avis s'inscrit dans le cadre de la gestion et du traitement des comportements inacceptables au sein et aux abords des domaines récréatifs et établit un cadre (légal) visant à punir ces comportements, basé sur la loi du 21 décembre 1998 *relative à la sécurité lors des matches de football*.

Bien que l'Autorité comprenne en principe la présente problématique, elle constate néanmoins que plusieurs adaptations du projet s'imposent.

La principale remarque à cet égard concerne la nécessité de déjà définir explicitement les modalités techniques et organisationnelles du contrôle de l'accès (et du système 'hit'/ 'no hit') dans le projet de façon à ce qu'aucun couplage n'ait lieu entre le contrôle de l'identité proprement dit et le registre central des sanctions et qu'il ne soit en aucun cas possible pour les exploitants du domaine et leurs préposés d'avoir une vue directe sur les données (à caractère personnel) qui sont enregistrées dans ce registre.

En outre, l'Autorité formule encore plusieurs remarques concernant la nécessité d'établir la qualité des exploitants de domaines, les définitions à appliquer pour certaines catégories de données à caractère personnel et (le moment où débutent) les délais de conservation des données à caractère personnel.

Enfin, l'Autorité se pose des questions majeures sur la proportionnalité et la nécessité du périmètre maximal établi autour des domaines récréatifs et la possibilité d'y intervenir avec une grande sévérité envers des personnes.

Pour une énumération exhaustive des remarques, l'Autorité renvoie au dispositif.

Le Service d'Autorisation et d'Avis de l'Autorité de protection des données (ci-après "l'Autorité"), présent.e.s : Mesdames Cédrine Morlière, Nathalie Ragheno et Griet Verhenneman et Messieurs Yves-Alexandre de Montjoye, Bart Preneel et Gert Vermeulen ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après "la LCA") ;

Vu l'article 43 du Règlement d'ordre intérieur selon lequel les décisions du Service d'Autorisation et d'Avis sont adoptées à la majorité des voix ;

Vu le 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, ci-après le "RGPD") ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après "la LTD") ;

Vu la demande d'avis de Monsieur Peter De Roover, Président de la Chambre des représentants, (ci-après : le demandeur), reçue le 4/11/2024 ;

Émet, le 30 janvier 2025, l'avis suivant :

I. OBJET DE LA DEMANDE D'AVIS

1. Le 4 novembre 2024, le demandeur a sollicité l'avis de l'Autorité au sujet des articles 14, 16, 20 – 21, 25 et 32 – 34 de la proposition de loi *relative à la sécurité dans les domaines récréatifs* (ci-après : le projet).

2. Cette proposition de loi reprend partiellement le texte des propositions DOC 53 2224/001, DOC 54 373/001 et DOC 55 3434/001, en tenant compte en particulier des avis déjà recueillis concernant la proposition DOC 55 3434/001. Enfin, il faut également se référer à cet égard à l'avis n° 18/2023[1] de l'Autorité concernant une proposition de loi *modifiant la nouvelle loi communale en vue de faciliter l'instauration d'une interdiction nationale d'accès aux domaines récréatifs*, avec pour principales critiques l'absence de définition claire de la notion de "domaine

[1] Consultable via le lien suivant : https://www.autoriteprotectiondonnees.be/publications/avis-n-18-2023.pdf.

récréatif", le manque de clarté quant à savoir à quelles conditions et dans quelles circonstances une personne peut être sanctionnée[2], l'encadrement insuffisant du rôle des exploitants de domaines récréatifs en matière de sanction et de contrôle des interdictions de domaine et des interdictions de périmètre et le nombre insuffisant de mesures prises pour garantir le respect du droit à la protection des données. Dans le présent avis, l'Autorité examine en particulier dans quelle mesure ces critiques ont été prises en compte.

3. Le projet se situe dans le cadre de la gestion et du traitement des comportements inacceptables au sein et aux abords des domaines récréatifs. Conformément aux développements du projet, le demandeur vise à instaurer un cadre obligeant les exploitants de domaines récréatifs à créer eux-mêmes une série de conditions de sécurité, telles que par exemple l'élaboration d'un règlement d'ordre intérieur[3]. Sont ensuite déterminés le champ d'application *ratione temporis* (les horaires durant lesquels il est possible d'infliger des sanctions administratives) et *ratione materiae* (les infractions passibles de sanctions). Concrètement en ce qui concerne les sanctions qui peuvent être infligées, l'on s'inspire de la loi du 21 décembre 1998 *relative à la sécurité lors des matches de football* (ci-après : la loi football), vu que le demandeur estime qu'il existe d'importantes similitudes entre les infractions visées dans les deux réglementations.[4]

4. Le projet définit également les modalités pour l'infliction d'avertissements officiels et de sanctions effectives ainsi que les règles (particulières) pour la notification de la décision, la formation d'un recours ainsi que les délais à respecter et les exceptions à cet égard.

5. Enfin, le Titre 7 du projet définit les règles en matière de traitement de données et d'échange d'informations. Dans ce contexte la création d'un registre centralisé des personnes physiques ayant fait l'objet d'une ou plusieurs sanctions visées dans le projet est envisagée. Ce registre est accessible aux fonctionnaires désignés par le Roi qui sont chargés de l'infliction de ces sanctions

---

[2] En particulier, la constatation selon laquelle la proposition de loi susmentionnée ne comportait aucune disposition sur les conditions et les circonstances dans lesquelles une personne pouvait être sanctionnée a donné lieu à une remarque fondamentale sur la licéité des traitements de données à caractère personnel visés. À la lumière des articles 7 et 8 de la de la Charte des droits fondamentaux de l'Union européenne et des articles 12 et 22 de la Constitution, le législateur ne peut pas se contenter, pour l'infliction de sanctions, de renvoyer au libre arbitre des exploitants de domaines récréatifs. Il incombe par contre au législateur, en tenant compte des principes de prévisibilité, de nécessité et de proportionnalité, de définir un cadre légal qui (1) détermine dans quelles circonstances et à quelle conditions une personne peut être sanctionnée et (2) qui impose aux exploitants de domaines récréatifs l'obligation d'assurer (prendre part à/au) l'application et le contrôle du respect des sanctions infligées. Voir en particulier les points 10 - 29 de l'avis n° 18/2023.

[3] En ce qui concerne l'obligation pour les exploitants de domaines d'élaborer un règlement d'ordre intérieur, il paraît indiqué de préciser explicitement que ce règlement doit reprendre au moins les infractions visées par le projet. Il semble en outre nécessaire de définir les conditions dans lesquelles l'exploitant peut, le cas échéant, aller au-delà de ce que prescrit le projet. En tout état de cause, les mesures prévues dans le règlement d'ordre intérieur doivent toujours être manifestement proportionnées et ne peuvent pas être de nature à discriminer *ab initio* certains groupes de population, de manière directe ou indirecte.

[4] Toutefois, dans ce contexte, l'Autorité se réfère à l'avis négatif n° 2024/3 de l'IFDH concernant la présente proposition de loi, qui conteste fortement la légitimité invoquée du lien avec la loi football. Voir : https://federaalinstituutmensenrechten.be/sites/default/files/2024-12/20241128_Advies%20recreatiedomeinen_2024_FR.pdf.

et (de manière limitée) aux exploitants et aux responsables de la sécurité des domaines récréatifs ainsi qu'aux personnes qu'ils désignent qui sont chargées du contrôle de l'accès.

II. EXAMEN QUANT AU FOND

a. Base juridique

6. *Rappel des principes :* Toute norme régissant le traitement de données à caractère personnel (et constituant par nature une ingérence dans le droit à la protection des données à caractère personnel) doit être nécessaire et proportionnée et répondre aux exigences de prévisibilité et de précision dans le chef des personnes concernées. En vertu de l'article 6.3 du RGPD, lu en combinaison avec les articles 22 de la *Constitution* et 8 de la CEDH, une telle norme légale doit définir les éléments essentiels des traitements allant de pair avec l'ingérence de l'autorité publique. Dans ce cadre, il s'agit au moins :
   - de la (des) finalité(s) précise(s) et concrète(s) des traitements de données ;
   - de la désignation du (des) responsable(s) du traitement (à moins que cela ne soit clair) ;

   Toutefois, si les traitements de données à caractère personnel allant de pair avec l'ingérence de l'autorité publique représentent une ingérence importante dans les droits et libertés des personnes concernées, la norme légale doit également définir les éléments essentiels (complémentaires) suivants :
   - les (catégories de) données à caractère personnel traitées qui sont pertinentes et non excessives ;
   - les catégories de personnes concernées dont les données à caractère personnel seront traitées ;
   - les catégories de destinataires des données à caractère personnel ainsi que les circonstances dans lesquelles ils reçoivent les données et les motifs y afférents ;
   - le délai de conservation maximal des données à caractère personnel enregistrées ;
   - l'éventuelle limitation des obligations et/ou des droits visé(e)s aux articles 5, 12 à 22 et 34 du RGPD.

7. *Application de ces principes* : Dans le cas présent, au vu de la nature et de l'ampleur des traitements de données envisagés, des (catégories de) personnes concernées et des (catégories de) données à caractère personnel à traiter, il est indubitablement question d'une ingérence importante dans les droits et libertés des personnes concernées. Il est en effet question de traitements ayant lieu à des fins de surveillance ou de contrôle, à savoir la sanction de personnes, dont, le cas échéant, des mineurs, qui commettent des infractions au sens du projet. L'identité de ces personnes ainsi que l'infraction (les infractions) sont enregistrées dans un registre central afin de permettre aux fonctionnaires sanctionnateurs et aux exploitants de domaines récréatifs de faire

appliquer les sanctions infligées (parmi lesquelles, par exemple, une interdiction de domaine ou de périmètre). Il est donc nécessaire que les éléments essentiels 'complémentaires' du traitement soient établis dans une norme légale formelle.

b. Finalité

8. Conformément à l'article 5.1.b) du RGPD, le traitement de données à caractère personnel ne peut être effectué que pour des finalités déterminées, explicites et légitimes.

9. Il a déjà été clarifié ci-avant que le projet se situe dans le contexte de la sanction de comportements inacceptables au sein et aux abords des domaines récréatifs[5] et du contrôle effectif du respect des sanctions infligées.

10. Tout d'abord, l'article 33, § 2 du projet dispose ce qui suit : "*§ 2. Le traitement des données visé au paragraphe 1er vise* ***à punir toute infraction éventuelle d'une sanction administrative****.*" . L'article 34, §§ 1 - 2 du projet spécifie ensuite : "*Toute décision imposant, en vertu de la présente loi, un avertissement, une amende administrative, une interdiction de domaine administrative, une interdiction de domaine judiciaire ou une interdiction de domaine à titre de mesure de sécurité est communiquée à un fonctionnaire désigné par le Roi, selon les modalités fixées par Lui par arrêté délibéré en Conseil des ministres.*
§ 2. Le fonctionnaire visé au paragraphe 1er ***tient un seul fichier des personnes physiques qui ont fait l'objet d'une ou de plusieurs sanctions visées au paragraphe 1er****. (…)*
Ce fichier vise à ***assurer la gestion des sanctions****.*"
Le paragraphe 5 de ce même article ajoute ce qui suit : *"Pour le contrôle du respect de l'interdiction de domaine administrative ou judiciaire infligée ou de l'interdiction de domaine imposée à titre de mesure de sécurité, l'exploitant et le responsable de la sécurité d'un domaine récréatif ont accès aux données à caractère personnel du registre en vue d'obtenir un résultat "hit/no hit" concernant la présence ou l'absence d'une interdiction de domaine imposée (...).*
Il y a un ***résultat "hit"*** *lorsque l'une des sanctions visées à l'alinéa 1er a été infligée. En cas de résultat "hit", la personne qui consulte le registre obtient la* ***confirmation de l'existence d'un résultat "hit", ainsi qu'une copie de la sanction infligée****.*
Il y a un ***résultat "no hit"*** *lorsqu'aucune sanction visée à l'alinéa 1er n'a été infligée. En cas de résultat "no hit", la personne qui consulte le registre* ***est informée qu'il y a un résultat "no hit"****.*
La consultation a lieu au travers d'un accès électronique dont les modalités sont fixées par le Roi.

[5] L'article 2, 1° du projet définit "domaine récréatif" comme suit : "*le domaine, accessible au public et* ***doté d'une enceinte*** *et d'infrastructures récréatives, défini par le Roi, qui est exploité à des fins de détente du public." Cette définition permet de délimiter le champ d'application concret du projet et répond ainsi à l'une des principales critiques formulées dans l'avis n° 18/2023 susmentionné.*

11. La finalité du traitement est donc double. Tout d'abord, les données à caractère personnel des contrevenants (potentiels) doivent être traitées afin de pouvoir constater les infractions et pouvoir ensuite les sanctionner (ou non)[6]. Ensuite, ces données seront enregistrées afin de permettre aux fonctionnaires sanctionnateurs et aux exploitants de domaines de contrôler effectivement le respect d'une interdiction de domaine ou de périmètre.

12. Bien que l'Autorité considère qu'il s'agit en principe de finalités déterminées, explicites et légitimes, elle estime néanmoins - malgré la délégation au Roi de préciser les modalités d'accès électronique au registre central des sanctions par les exploitants de domaines - qu'il convient de développer davantage ou de préciser les modalités du système 'hit/ no hit' dans le projet, ou du moins dans les développements. En effet, les modalités de mise en œuvre du contrôle touchent intrinsèquement au caractère légitime et à la proportionnalité espérée des finalités. Dans le présent contexte, il est particulièrement important de préciser à cet égard les modalités du contrôle et plus précisément, s'il aura lieu de façon purement aléatoire [7]ou bien systématique [8](l'aspect organisationnel). Sur le plan technique, le contrôle s'effectue par la présentation et la lecture de la carte d'identité du visiteur concerné afin de vérifier s'il figure dans le registre central et, plus précisément, si une interdiction de domaine ou de périmètre lui a été infligée.

13. Comme expliqué de manière circonstanciée dans l'avis n° 18/2023, il peut suffire à cet effet que le fonctionnaire désigné par le Roi mette le registre des sanctions à disposition sous la forme d'une liste reprenant les données d'identification hachées des personnes concernées, fournie avec un filtre Cuckoo. Un filtre Cuckoo est un fichier de filtrage généré régulièrement (par exemple quotidiennement ou hebdomadairement) sur la base des données d'identité hachées de toutes les personnes auxquelles une sanction a été infligée et qui peuvent se voir refuser l'accès au domaine récréatif. Lors du contrôle de l'accès, la carte d'identité de la personne concernée est croisée ou comparée avec le fichier filtre à l'aide d'un programme, ce qui produit un résultat 'hit' ou 'no hit'. Le filtre peut encore être affiné s'il était souhaitable d'afficher non seulement l'existence d'une sanction active, mais aussi la nature de la sanction[9] et le mois ou la semaine où la sanction expire. Compte tenu du fait que l'eID de la personne concernée doit de toute façon être présentée lors du contrôle de l'accès, l'Autorité estime que la mention de la nature de la sanction (et, le cas

[6] L'article 23 du projet prévoit en effet un délai de prescription de six mois pour l'imposition d'une sanction administrative à compter du jour où le fait est commis, les éventuelles procédures de recours non comprises.

[7] Dans ce cas, il existe en effet un risque important de discrimination envers certains groupes qui sont systématiquement - à tort ou raison - associés à des comportements problématiques au sein et aux abords des domaines récréatifs.

[8] Vu que le projet définit un domaine récréatif comme un domaine doté d'une enceinte, mais accessible au public, il est possible en l'espèce d'opter pour un contrôle d'identité systématique à l'entrée.

[9] Dans ce cas, il peut toutefois uniquement s'agir d'une interdiction de domaine administrative ou judiciaire ou d'une interdiction de domaine imposé en tant que mesure de sécurité. L'existence d'une amende administrative ne constitue en effet pas un motif d'exclusion valable.

échéant, de son délai d'expiration) peut suffire, en cas de résultat 'hit', à vérifier la légitimité d'un refus d'accès par le contrôleur, mais aussi à le motiver à l'égard du visiteur refusé.

14. L'Autorité observe en outre que lors du contrôle de l'accès, aucune journalisation ne peut avoir lieu sur le dispositif qui lit la carte d'identité et transmet les informations au programme.

15. La méthode de travail décrite ci-dessus permet d'empêcher que le service qui gère le registre central des sanctions reçoive des informations relatives à l'identité des visiteurs d'un domaine récréatif, vu que la procédure de vérification s'effectue entièrement au niveau local et hors ligne (autrement dit, aucun couplage n'a lieu entre les résultats du contrôle de l'accès et le registre central). En outre, cette méthode permet d'éviter que l'exploitant du domaine (ou ses préposés) ai(en)t directement accès aux données à caractère personnel dans le registre (en effet, le programme permet uniquement de vérifier si un visiteur spécifique (dont les données sont connues) apparaît ou non sur la liste). Afin de permettre une certaine forme de contrôle *ex post*[10], il est par contre acceptable que le programme rapporte au service (le responsable du traitement du registre) la fréquence d'utilisation (par jour ou par semaine) et le nombre de 'hits'.

16. À cet égard, il est encore recommandé de préciser la procédure à suivre lorsqu'il est constaté à l'entrée d'un domaine récréatif que le visiteur présente une eID qui ne lui appartient manifestement pas ou ne dispose pas d'une carte d'identité belge (par exemple les touristes). Il convient également de consacrer une attention particulière à la protection des données de journalisation des utilisateurs, par exemple lorsqu'un ticket d'entrée peut être acheté en ligne et qu'une vérification a déjà lieu à ce moment-là (via un lecteur d'eID ou itsme). Enfin, le projet doit prévoir une possibilité de contrôle en cas de suspicion d'enregistrement erroné dans le registre central des sanctions[11] (ce qui donnerait lieu à un refus d'accès injustifié). L'existence d'une telle possibilité et ses modalités doivent être reprises dans le règlement d'ordre intérieur et doivent pouvoir être consultées à chaque endroit où un contrôle d'identité peut avoir lieu.

17. De manière générale, l'Autorité fait encore remarquer qu'un éventuel contrôle systématique de l'identité constituerait une ingérence dans les droits fondamentaux des personnes qui accèdent ou souhaitent accéder à un domaine récréatif et qu'il convient par conséquent de veiller en tout temps à l'équilibre entre l'importance de maintenir/garantir la tranquillité et l'ordre publics au sein des domaines récréatifs d'une part et les droits fondamentaux des personnes concernées en matière de respect de la vie privée et de protection des données, d'autre part. S'il s'agit par contre de contrôles sélectifs ou aléatoires, il convient de se montrer particulièrement attentif au risque

[10] Par exemple pour détecter l'utilisation abusive (ou la non utilisation) du système.

[11] L'Autorité souligne qu'il ne s'agit pas ici d'une procédure de recours supplémentaires contre des sanctions imposées et passées en force de chose jugée.

accru de discrimination. À cette fin, il est nécessaire de prendre des dispositions au moins au niveau interne (le cas échéant, par le biais des lignes directrices internes de chaque domaine récréatif) afin de veiller à ce que le contrôle de l'accès repose sur une base objective et que son caractère aléatoire soit établi et démontrable.

c. Responsable du traitement

18. Conformément à l'article 4.7) du RGPD, le responsable du traitement est toute personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre. Dans un souci d'exhaustivité, l'Autorité rappelle que la désignation du responsable du traitement doit être adéquate au regard des circonstances factuelles. Tant le Comité européen de la protection des données que l'Autorité ont insisté sur la nécessité d'approcher ces concepts dans une perspective factuelle. Il est donc nécessaire de désigner la ou les entités qui, dans les faits, poursui(ven)t la finalité du traitement visé et en assure(nt) la maîtrise.

19. L'Autorité fait également remarquer qu'en cas de responsabilité conjointe du traitement, l'article 26 du RGPD s'applique et pour les conséquences pratiques, elle renvoie au point 2 de la deuxième partie des lignes directrices 07/2020 établies le 2 septembre 2020 par le Comité européen de la protection des données *concernant les notions de responsable du traitement et de sous-traitant dans le RGPD.*[12] Il conviendra notamment de définir de manière transparente qui est responsable pour répondre aux personnes concernées qui souhaitent exercer les droits qui leur sont conférés dans le cadre du RGPD (sans préjudice du fait que conformément à l'article 26.3 du RGPD, les personnes concernées peuvent exercer leurs droits dans le cadre du RGPD vis-à-vis de chacun des responsables conjoints du traitement).

20. Tout d'abord, l'article 33, § 3 du projet prévoit ce qui suit : *"Le service du fonctionnaire visé à l'article 16, § 1er, alinéa 1er, est compétent pour le traitement de ces données à caractère personnel."* Il s'agit notamment des données traitées par le fonctionnaire désigné par le Roi en vue de sanctionner d'éventuelles infractions au moyen d'une sanction administrative (le fonctionnaire sanctionnateur). Il ressort des développements que par analogie avec la loi football, ce service sera le SPF Intérieur. Il est possible que ce soit l'actuelle cellule football qui sera concrètement chargée de cette mission.

[12] À consulter via le lien suivant (attention : cette traduction n'a pas encore été validée officiellement) : https://edpb.europa.eu/system/files/2023-10/eppb_guidelines_202007_controllerprocessor_final_fr.pdf.

21. L'article 34, § 2 du projet dispose ensuite ce qui suit : *"Le fonctionnaire visé au paragraphe 1er tient un seul fichier des personnes physiques qui ont fait l'objet d'une ou de plusieurs sanctions visées au paragraphe 1er. Le service pour lequel travaille le fonctionnaire est responsable du traitement de ce fichier."*

22. À cet égard, l'Autorité estime qu'en ce qui concerne la constatation et la sanction des infractions, ainsi que l'enregistrement des infractions dans le registre central des sanctions, la désignation du service (SPF Intérieur) comme responsable du traitement correspond au rôle que cet acteur assumera dans la pratique. Néanmoins, il est recommandé de déjà y définir également la qualité concrète des exploitants de domaines. En vertu du projet, certaines obligations et compétences sont en effet imposées / attribuées aux exploitants de domaines. Les exploitants (ou leurs préposés) doivent élaborer un règlement d'ordre intérieur[13] et contrôler le respect des interdictions de domaines imposées, contrôle dans le cadre duquel ils doivent traiter certaines données de leurs visiteurs et, en outre, pouvoir accéder (de façon indirecte et limitée) au registre des sanctions, conformément à l'article 34, § 5 du projet. Pour ces finalités de traitement, il convient donc de vérifier s'il est question d'une responsabilité unique ou conjointe, ou bien d'une relation de sous-traitance au sens de l'article 28 du RGPD[14]. En fonction de la qualification concrète, les dispositions respectives du RGPD devront être prises en compte.

23. Dans ce contexte, il convient de souligner que les dispositions du projet, et plus précisément la désignation du SPF Intérieur en tant que responsable du traitement pour la sanction d'éventuelles infractions et la gestion du registre des sanctions, n'affectent pas la responsabilité des agents de surveillance (externes), des services de police (locale) (les verbalisants) et, le cas échéant, du ministère public pour les traitements de données qu'ils effectuent dans le cadre de leurs missions légales.

24. Enfin (à titre plutôt rédactionnel), eu égard à la constatation selon laquelle le terme 'responsable du traitement' est utilisé à plusieurs reprises dans le projet, l'Autorité recommande de désigner explicitement le service concerné (à savoir le SPF Intérieur) en tant que responsable du traitement à l'article 33, § 3 du projet.[15] Actuellement, il est simplement indiqué que le service précité est compétent pour les traitements de données visés. Cela occasionne des problèmes d'interprétation, en particulier à la lecture de l'article 34 du projet, en vertu duquel les exploitants de domaines

[13] Voir aussi la note de bas de page 3 ci-avant.

[14] Ceci n'affecte évidemment pas la responsabilité des exploitants de domaines pour les traitements de données qui peuvent avoir lieu, le cas échéant, dans le cadre de la gestion et de l'exploitation normales des domaines récréatifs (logistique, RH...).

[15] À cet égard, il convient de faire remarquer que les développements de l'article 33 du projet indiquent que le fonctionnaire sanctionnateur agit en tant que responsable du traitement. Ceci est contraire au texte de l'article 33 du projet, ainsi qu'avec l'esprit des développements de l'article 16 du projet. Le passage en question doit dès lors être utilement modifié.

doivent communiquer certaines données au "responsable du traitement". Dans ce contexte, il est donc crucial que l'identité du responsable du traitement soit établie sans ambiguïté.

d. Proportionnalité/Minimisation des données

25. L'article 5.1.c) du RGPD prévoit que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités visées (principe de 'minimisation des données').

26. À cet égard, il convient de faire une distinction entre le traitement de données à caractère personnel de visiteurs et de (potentiels) contrevenants d'une part (tant en ce qui concerne l'infliction de sanctions en soi que la mention dans le registre central des sanctions) et le traitement de données à caractère personnel de certains collaborateurs des exploitants de domaines, d'autre part.

27. Tout d'abord, l'article 33, § 1er, alinéa 1er du projet, qui se rapporte aux traitements effectués en vue de sanctionner d'éventuelles infractions, dispose ce qui suit : *"Dans le cadre de l'application de la présente loi, les données à caractère personnel suivantes peuvent être traitées : les données d'identification du contrevenant, notamment ses nom, prénoms et date de naissance, son lieu de résidence principal, son numéro de registre national, les données relatives à la capacité et à la représentation et les données relatives à la tutelle et la filiation.*

28. En ce qui concerne les nom, prénoms, date de naissance et lieu de résidence principal, l'Autorité ne formule aucune remarque particulière.

29. En ce qui concerne le traitement du numéro de Registre national, l'Autorité reconnaît l'importance d'une identification correcte et du traitement de données qui répondent aux exigences de qualité et d'exactitude. Elle souligne toutefois que l'utilisation du numéro de Registre national en Belgique est strictement régie par l'article 8 de la loi du 8 août 1983 *organisant un registre national des personnes physiques*. L'Autorité rappelle également de manière générale que les numéros d'identification uniques bénéficient d'une protection particulière. L'article 87 du RGPD prévoit que les États membres qui définissent un numéro d'identification national doivent veiller à ce qu'il ne soit utilisé que sous réserve de garanties appropriées pour les droits et libertés de la personne concernée. Ainsi, la Commission de la protection de la vie privée, prédécesseur en droit de l'Autorité, a déjà attiré précédemment[16] l'attention sur le respect des conditions suivantes en la matière :

[16] Voir l'avis n° 19/2018 du 29 février 2018 sur un *avant-projet de loi portant des dispositions diverses "Intérieur"*.

- l'utilisation d'un numéro d'identification général doit être limitée aux cas où il est strictement nécessaire étant donné que son utilisation implique des risques en termes d'interconnexion de fichiers ;
- les finalités doivent être précisées clairement et explicitement afin que l'on puisse entrevoir/prévoir les types de traitements visés ;
- la durée de conservation et les éventuelles communications à des tiers doivent également être encadrées ;
- des mesures techniques et organisationnelles doivent encadrer adéquatement l'utilisation sécurisée ; et
- le non-respect des dispositions encadrant l'utilisation doit être sanctionné au moyen de sanctions effectives, proportionnées et dissuasives.

30. À cet égard, l'Autorité se demande s'il n'est pas indiqué de mentionner également le numéro *bis*, étant donné que tous les contrevenants ne disposeront pas nécessairement d'un numéro de Registre national.

31. L'Autorité estime en outre qu'il est également nécessaire de clarifier ce que recouvre concrètement la notion de "capacité" et dans quel but cette information sera traitée. La capacité peut en effet être liée à l'âge (moins de quatorze ans, entre quatorze et dix-huit ans ou majeur), mais aussi à la capacité juridique (non liée à l'âge) de la personne concernée. Cette distinction est importante car si seule cette dernière catégorie est visée, il sera le cas échéant question d'un traitement de données à caractère personnel liées à la santé ou de données à caractère personnel autrement sensibles, qui bénéficient d'une protection particulière en vertu de l'article 9.1 du RGPD, et dont le traitement est uniquement possible à condition de pouvoir invoquer un des motifs d'exception visés à l'article 9.2 du RGPD. Dans le présent contexte, le traitement de telles données ne peut être légitime que s'il est absolument et manifestement nécessaire à l'appréciation concrète d'une situation particulière[17]. Par exemple, si l'incapacité juridique de la personne concernée a pour conséquence qu'il ne soit pas question d'une infraction au sens du projet, ou si elle donne lieu à des circonstances atténuantes. En tout état de cause, l'Autorité demande que les notions d' 'âge' et de 'capacité' soient reprises séparément dans le projet et que la manière dont la notion de 'capacité' doit être interprétée soit explicitement précisée, par exemple dans les développements.

32. Enfin, en ce qui concerne les '*données relatives à la tutelle et la filiation*', l'Autorité estime nécessaire de préciser dans les développements que dans le présent contexte, 'filiation' se rapporte uniquement à l'établissement de la parentalité et d'ajouter, par analogie avec l'article 34,

[17] Cela signifie que ces données ne peuvent être traitées qu'en ordre secondaire, lorsqu'il peut être déduit d'une situation concrète que la (l'in)capacité (de l'une) des personnes concernées constitue un élément essentiel pour l'évaluation de la gravité des faits ou la fixation de la peine.

§ 3, 1er alinéa du projet[18], la partie de phrase suivante : "*… **dans le cas d'un mineur**, les données relatives à la tutelle et à la filiation.*"

33. L'article 34, § 3, 1er alinéa du projet détermine ensuite quelles données sont reprises dans le registre central des sanctions : "*§ 3. Ce fichier contient les données à caractère personnel et les informations suivantes :*
    1° *les nom, prénoms et date de naissance, et la résidence principale des personnes qui font l'objet de sanctions ; s'il s'agit d'un mineur, les noms, prénoms et date de naissance, et la résidence de chaque titulaire qui exerce l'autorité parentale sur le mineur ;*
    2° *la nature des faits commis ;*
    3° *la nature de la sanction, ainsi que le jour où elle a été infligée ;*
    4° *les sanctions qui ne sont plus susceptibles de recours."*

34. Bien qu'à la lumière de ce qui a déjà été expliqué ci-dessus, les catégories de données susmentionnées n'appellent aucune remarque particulière (supplémentaire), l'Autorité estime que, en vue du contrôle *ex post* du respect des interdictions de domaine ou de périmètre, il est néanmoins nécessaire d'enregistrer également dans le registre le numéro de registre national ou le numéro *bis* du contrevenant. En effet, dans la mesure où ce contrôle s'effectue par la présentation et la lecture de la carte d'identité de la personne concernée, le numéro de Registre national ou le numéro *bis* constitue la donnée par excellence pour obtenir, après croisement avec le fichier central, un résultat *'hit / no hit'*. Il convient de modifier utilement le projet en ce sens. Il paraît en outre indiqué de préciser que la photo de la personne concernée (sur la carte d'identité) peut également être traitée, notamment en vue du contrôle de l'accès (premièrement afin de pouvoir établir que la personne figurant sur la photo est la même que celle qui présente son eID pour le contrôle).

35. Deuxièmement, les données d'identification de certains collaborateurs des exploitants de domaines sont également traitées. À cet égard, l'article 34, § 5 du projet dispose ce qui suit : "§ 5. *L'exploitant et le responsable de la sécurité d'un domaine récréatif peuvent déléguer aux personnes, nommément désignées par écrit et chargées du contrôle de l'accès, leur accès au registre. Cette délégation doit être motivée et justifiée par les nécessités du service. La liste de ces personnes nommément désignées doit être communiquée sans délai par l'exploitant et le responsable de la sécurité au responsable du traitement. La liste des personnes qui ont ainsi accès au registre doit être tenue à disposition de l'Autorité de protection des données par le responsable du traitement. Le responsable du traitement doit veiller à ce que les personnes désignées soient tenues au respect du caractère confidentiel des données concernées."*

[18] Voir aussi ci-dessous les points 33 e.s.

36. À cet égard, à des fins de journalisation et de suivi des contrôles d'identité, il semble justifié de tenir une liste des personnes chargées du contrôle de l'accès et de tenir cette liste à la disposition de l'Autorité. Ceci ne porte toutefois pas préjudice à ce qui est exposé au point 13, à savoir que l' 'accès' au registre central des sanctions par les exploitants de domaines ou leurs préposés doit rester limité aux données hachées des personnes concernées, où après lecture de l'eID, seul un résultat 'hit' avec mention de la nature de la sanction ou un résultat 'no hit' s'affiche.

37. Enfin - dans la mesure où **le périmètre** autour du domaine récréatif **implique une zone au sein de laquelle les données à caractère personnel de toute personne pourraient être traitées en vue d'atteindre les finalités visées dans le projet** -, l'Autorité exprime sa préoccupation plus générale concernant la légitimité et le caractère justifié de la possibilité, dans le contexte du projet, d'infliger des sanctions dans ce périmètre, lequel est fixé à **un rayon maximal de 1.000 mètres** à partir de l'enceinte du domaine récréatif. L'Autorité considère qu'un rayon aussi vaste est insuffisamment (lire : n'est pas) légitime et soulève donc, à plusieurs égards, des interrogations sur la proportionnalité de ces mesures, en particulier compte tenu de l'arrêt n° 44/2015 de la Cour constitutionnelle dans lequel la Cour a estimé - en ce qui concerne l'interdiction de lieu[19] - que celle-ci n'est compatible avec la liberté de circulation personnelle que dans la mesure où le périmètre en question n'est pas plus vaste que nécessaire pour empêcher ou mettre un terme aux troubles de l'ordre public. Une interdiction de périmètre qui peut s'étendre jusqu'à 1.000 mètres au-delà des limites extérieures du domaine récréatif va bien au-delà de ce qui est nécessaire pour "*éviter que les troubles ne se déplacent en dehors des limites du domaine récréatif*" - une finalité qui peut d'ailleurs tout aussi bien être poursuivie en recourant aux compétences de police normales dont disposent les bourgmestres en vertu de la Nouvelle loi communale.[20]

38. Premièrement, l'Autorité estime qu'en l'espèce, il ne peut y avoir aucune comparaison entre la loi football d'une part et la sécurité des domaines récréatifs, d'autre part. En effet, les mesures relatives au périmètre prévues dans la loi football visent (en premier lieu) à protéger des ((dizaines de) milliers de) supporters et les membres des forces de l'ordre qui se trouvent à proximité d'un stade avant ou après un match de football, ou à intercepter à temps les bus organisés transportant des hooligans pour établir l'identité de leurs occupants. L'interdiction de périmètre dans la loi football est en outre beaucoup plus limitée dans le temps : elle s'applique à partir de cinq heures avant le début du match de football et se termine cinq heures après[21]. Ces finalités ne peuvent donc pas être invoquées *mutatis mutandis* comme motif de justification dans le présent contexte.

[19] Article 134*sexies* de la Nouvelle loi communale.

[20] Voir par exemple l'article 133, premier alinéa et l'article 135, § 2 de la Nouvelle loi communale.

[21] Article 24, § 1er, alinéa 3 de la loi football.

Il va également de soi que la simple mention dans les développements de l'article 2 du projet que "*les incidents observés au cours des dernières années dans les domaines récréatifs se sont également produits à l'extérieur de l'enceinte de ces domaines*" peut difficilement justifier la portée de certaines mesures.

39. Deuxièmement - compte tenu à nouveau du périmètre particulièrement vaste qui est établi -, l'Autorité se demande comment le fonctionnaire verbalisateur doit démontrer le lien entre les infractions visées aux articles 6 (le jet d'objets) et 11 (l'incitation à la haine ou à la violence) du projet et le maintien de la sécurité dans les domaines récréatifs. De telles infractions peuvent en effet déjà être sanctionnées actuellement, sans qu'il soit nécessaire que le contrevenant concerné agisse avec l'intention de semer la pagaille au sein ou aux abords du domaine récréatif. Dans la mesure où à la suite de tels faits, une interdiction de domaine ou de périmètre serait imposée, le rapport avec le domaine (la sécurité du domaine) récréatif doit être indubitablement établi et démontrable.

40. Troisièmement, l'Autorité attire l'attention sur les conditions strictes qui, en vertu du chapitre 3 de la loi du 2 octobre 2017 *réglementant la sécurité privée et particulière*, s'appliquent aux services internes de gardiennage. À cet égard, l'Autorité rappelle que conformément à l'article 24, quatrième alinéa *j°* l'article 115, 2° de la même loi, sur la voie publique (lisez : dans le périmètre du domaine récréatif), les agents de gardiennage de tels services (**agréés**) peuvent uniquement exercer des activités de gardiennage relatives au gardiennage d'événements. Ceci est difficilement compatible avec l'article 8 du projet, qui dispose ce qui suit : *"(...) peut encourir une ou plusieurs sanctions visées aux articles 12 et 13, quiconque ne respecte pas dans le domaine récréatif ou* ***le périmètre*** *les directives ou injonctions données par un agent de gardiennage ou* ***un membre du service interne de gardiennage*** *dans l'exercice de ses tâches (...)"* Un tel pouvoir nécessiterait en effet (au minimum) que l'agent de gardiennage concerné (du service interne) soit en mesure de faire produire aux personnes des documents d'identité (en dehors du cadre du contrôle de l'accès) ou de s'en saisir et, en attendant l'arrivée de la police, de les empêcher de s'enfuir. Il est donc évident que l'article 8 du projet doit être modifié en profondeur, en fonction des prescriptions de la loi précitée.

41. En résumé, l'Autorité estime qu'il est nécessaire de revoir en profondeur à la fois l'étendue du périmètre ainsi que la nature et la gravité des sanctions possibles à cet égard et de les motiver explicitement dans les développements. En effet, à l'heure actuelle, l'Autorité se voit contrainte de donner un avis résolument négatif sur cet aspect du projet.

e. Délai de conservation

42. En vertu de l'article 5.1.e) du RGPD, les données à caractère personnel ne peuvent pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées.

43. Tout d'abord, l'article 33, § 4 du projet prévoit ce qui suit : "*Les données à caractère personnel sont conservées pendant une période qui, au maximum, est égale au délai de conservation des données dans le registre conformément à l'article 34.*[22]*Les données à caractère personnel sont conservées au maximum pendant la période durant laquelle une sanction administrative peut être infligée conformément à l'article 23*[23]*. Si une sanction administrative est effectivement infligée, les délais de conservation de l'article 34 sont appliqués. En tout état de cause, les données à caractère personnel ne peuvent être conservées plus longtemps que nécessaire au regard des finalités pour lesquelles elles sont traitées.*[24]*"*

44. L'article 34, § 3, alinéa 2 du projet dispose à son tour ce qui suit : *"Les données visées à l'alinéa 1*[er] *sont conservées pendant cinq ans à compter du jour où la sanction a été infligée. Passé ce délai, elles sont soit détruites, soit anonymisées."*

45. L'Autorité estime qu'un tel délai se justifie à la lumière de la durée maximale d'une interdiction de domaine ou de périmètre (à savoir cinq ans) et du délai de conservation actuellement en vigueur pour les sanctions administratives communales. Néanmoins, il paraît indiqué dans ce cas de faire débuter le délai de conservation à partir du moment où la sanction est coulée en force de chose jugée (après l'expiration du délai de recours, ou après épuisement de toutes les voies de recours), afin qu'aucune confusion ne subsiste quant au moment où la sanction a été infligée.

46. Un tel délai de conservation ne porte toutefois pas préjudice au fait qu'après l'expiration d'une interdiction de domaine, il ne peut en aucun cas être possible pour l'exploitant de domaine ou ses préposés de prendre connaissance de l'existence de cette interdiction de domaine[25].

---

[22] Il manque un point à cette phrase dans le projet.

[23] L'article 23 régit le délai de prescription pour les (la sanction des) infractions administratives. L'action administrative s'éteint à l'issue d'un délai de six mois, à compter du jour où l'infraction a été commise. Cela implique que si aucune sanction n'a été infligée dans les six mois qui suivent la commission de l'infraction, toutes les données à caractère personnel collectées dans ce contexte doivent être détruites (ou anonymisées) sans délai.

[24] À titre purement rédactionnel, l'Autorité estime que les modifications suivantes au paragraphe susmentionné s'imposent :

- supprimer la première phrase, car elle n'apporte aucune plus-value juridique par rapport au reste du paragraphe ;
- à la deuxième phrase, par analogie avec les développements du projet, ajouter ce qui suit : *"Dans les cas où aucune sanction administrative n'est imposée, les données à caractère personnel sont conservées au maximum (...) conformément à l'article 23."* ;
- supprimer la quatrième et dernière phrase, car elle concerne une violation de l'interdiction de retranscription du RGPD, et n'apporte en outre aucune plus-value par rapport à l'article 5.1.e) du RGPD.

[25] Lorsqu'un visiteur souhaite à nouveau accéder à un domaine récréatif après l'expiration de l'interdiction de domaine qui lui a été imposée, le contrôle de l'accès ne doit générer qu'un résultat '*no hit*' , sans plus.

47. Pour les données qui sont traitées par la police et la justice, on peut évidemment renvoyer aux délais de conservation qui leur sont applicables, conformément à leur législation-cadre respective.

48. Deuxièmement, l'Autorité constate qu'aucun délai de conservation n'est établi pour les données d'identification des préposés au contrôle de l'accès. Il est nécessaire de fixer un délai de conservation maximal pour ces données également. Ce délai de conservation ne peut en aucun cas être plus long que les délais de conservation établis pour les données de journalisation (*infra*)).

49. Enfin, l'Autorité formule plusieurs remarques concernant les délais de conservation établis pour les données de journalisation en vertu respectivement des articles 33, § 5 et 34, § 6 du projet :
    - vu que les traitements de données visés à l'article 33 du projet concernent en premier lieu la constatation et la sanction effectives des infractions, l'Autorité se demande quelles consultations doivent faire l'objet de la journalisation prescrite[26]. Il est recommandé de préciser cet aspect. L'Autorité se demande également quel est le motif de justification pour le délai de conservation de cinq ans, à compter de l'expiration du délai de conservation visé à l'article 33, § 4 du projet. L'expiration de ce dernier délai implique en effet qu'aucune sanction n'a été imposée, ou que la sanction en question a été exécutée, qu'il n'existe plus la moindre voie de recours et que les données à caractère personnel concernées ont été détruites ou anonymisées. En tant que tel, l'Autorité ne voit pas quelle est la valeur ajoutée de ce délai de conservation supplémentaire pour les données de journalisation et demande qu'il soit raccourci de manière appropriée[27];
    - en ce qui concerne le délai de conservation des fichiers de journalisation visés à l'article 34, 1er alinéa, 2° du projet[28], l'Autorité estime également que des précisions s'imposent. Actuellement, on a l'impression que les fichiers de journalisation seront conservés indéfiniment, tant que le registre central des sanctions est tenu, ce qui permet difficilement de réussir le test de proportionnalité. Par analogie avec les arguments développés au tiret précédent, l'Autorité estime qu'un délai de conservation (pour les fichiers de journalisation) de deux ans maximum après la suppression définitive d'un dossier du fichier central peut largement suffire.

PAR CES MOTIFS,
l'Autorité,

[26] Sauf erreur, il n'est en effet pas encore question à l'heure actuelle d'un enregistrement dans le registre central, ce qui soulève la question de savoir sur quoi portent (doivent porter) les fichiers de journalisation.

[27] Un délai de conservation supplémentaire pour les fichiers de journalisation de 2 ans après l'expiration du délai de conservation initial semble en l'espèce pouvoir largement suffire.

[28] L'article 34, § 6, alinéa 3 du projet prévoit ce qui suit : *Le délai de conservation des fichiers de journalisation visés à l'alinéa 1er, 2°, est de cinq ans maximum, à compter du dernier traitement effectué dans le registre. (…)"*

estime que les modifications suivantes s'imposent dans le projet :

- préciser davantage les modalités du système '*hit / no hit*' conformément à ce qui est exposé aux points 12 – 17 ;
- définir la qualité de l'exploitant de domaine dans le cadre du contrôle de l'accès et de la 'consultation' du registre central des sanctions 22) ;
- désigner explicitement le service qui est responsable du traitement (point 24) ;
- outre le numéro de Registre national, mentionner également le numéro *bis* (point 30) ;
- préciser la notion de 'capacité' (point 31) ;
- préciser que la notion de 'filiation' concerne uniquement l'établissement de la parentalité (point 32) ;
- reprendre également le numéro de Registre national et le numéro *bis*, ainsi que la photo de la personne concernée dans les catégories de données à caractère personnel qui seront traitées (point 34) ;
- revoir l'étendue du périmètre ainsi que la nature et la sévérité des sanctions qui peuvent être infligées au sein du périmètre, à la lumière de ce qui est exposé aux points 37 – 41 ;
- préciser que le délai de conservation pour les données à caractère personnel débute au moment où la sanction est coulée en force de chose jugée (point 45) ;
- établir un délai de conservation (maximal) pour la liste des personnes chargées du contrôle de l'accès 48 ;
- revoir les dispositions en matière de délais de conservation pour les fichiers de journalisation conformément à ce qui est exposé au point 49.

Pour le Service d'Autorisation et d'Avis,
Cédrine Morlière, Directrice