Publicatieblad
van de Europese Unie

NL
L-serie

2026/1778

17.7.2026

UITVOERINGSVERORDENING (EU) 2026/1778 VAN DE COMMISSIE

van 16 juli 2026

tot vaststelling van de uitvoeringsregelingen voor het register van digitale productpaspoorten dat is opgezet uit hoofde van Verordening (EU) 2024/1781 van het Europees Parlement en de Raad

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) 2024/1781 van het Europees Parlement en de Raad van 13 juni 2024 betreffende de totstandbrenging van een kader voor het vaststellen van vereisten inzake ecologisch ontwerp voor duurzame producten, tot wijziging van Richtlijn (EU) 2020/1828 en Verordening (EU) 2023/1542, en tot intrekking van Richtlijn 2009/125/EG ([1]), en met name artikel 13, lid 5, tweede alinea, in samenhang met artikel 13, lid 5, derde alinea,

Overwegende hetgeen volgt:

(1) De Commissie moet op grond van artikel 13, lid 1, van Verordening (EU) 2024/1781 een digitaal register voor het digitale productpaspoort ("het register") opzetten om ten minste de unieke identificatiecodes op veilige wijze bij te houden. De belangrijkste componenten van het register moeten worden vastgesteld, evenals de technische en operationele rollen en verplichtingen van de marktdeelnemers die in het kader van het register van digitale productpaspoorten een product in de handel brengen of in gebruik nemen, de bevoegde nationale autoriteiten en douaneautoriteiten, en de Commissie. Voorts moet een logboeksysteem worden ingericht om de verrichtingen en interacties in het register te registreren en te monitoren teneinde de verantwoordingsplicht van alle gebruikers te waarborgen, en om de verantwoordelijkheid voor het onderhoud, de werking en de beveiliging van het register af te bakenen. Deze uitvoeringsregelingen omvatten ook regels met betrekking tot het gebruik van het register die van toepassing zijn op actoren in de waardeketen, bevoegde nationale autoriteiten en douaneautoriteiten, en de Commissie. In voorkomend geval moeten de bevoegde nationale autoriteiten de status van het digitale productpaspoort kunnen updaten of wijzigen op basis van de controles die zij uitvoeren overeenkomstig hun taken uit hoofde van de toepasselijke Uniewetgeving en de met de Uniewetgeving in overeenstemming zijnde nationale wetgeving.

(2) Het register moet informatie verstrekken over producten die vallen onder gedelegeerde handelingen die zijn vastgesteld op grond van Verordening (EU) 2024/1781, voor zover daarin voorzien wordt in het gebruik van een digitaal productpaspoort, en over batterijen, op grond van Verordening (EU) 2023/1542 van het Europees Parlement en de Raad ([2]). Ook andere wetgeving van de Unie kan vereisen dat informatie over producten in het register wordt opgeslagen. Dat is reeds het geval voor bouwproducten die binnen het toepassingsgebied van Verordening (EU) 2024/3110 van het Europees Parlement en de Raad ([3]) vallen, speelgoed dat binnen het toepassingsgebied van Verordening (EU) 2025/2509 van het Europees Parlement en de Raad ([4]) valt en detergenten en oppervlakteactieve stoffen voor eindgebruikers die binnen het toepassingsgebied van Verordening (EU) 2026/405 van het Europees Parlement en de Raad ([5]) vallen. Wanneer in andere wetgeving van de Unie wordt verwezen naar het

([1]) PB L, 2024/1781, 28.6.2024, blz.1, ELI: http://data.europa.eu/eli/reg/2024/1781/oj.

([2]) Verordening (EU) 2023/1542 van het Europees Parlement en de Raad van 12 juli 2023 inzake batterijen en afgedankte batterijen, tot wijziging van Richtlijn 2008/98/EG en Verordening (EU) 2019/1020 en tot intrekking van Richtlijn 2006/66/EG (PB L 191 van 28.7.2023, blz. 1, ELI: http://data.europa.eu/eli/reg/2023/1542/oj).

([3]) Verordening (EU) 2024/3110 van het Europees Parlement en de Raad van 27 november 2024 tot vaststelling van geharmoniseerde regels voor het verhandelen van bouwproducten en tot intrekking van Verordening (EU) nr. 305/2011 (PB L, 2024/3110, 18.12.2024, ELI: http://data.europa.eu/eli/reg/2024/3110/oj).

([4]) Verordening (EU) 2025/2509 van het Europees Parlement en de Raad van 26 november 2025 betreffende de veiligheid van speelgoed en tot intrekking van Richtlijn 2009/48/EG (PB L, 2025/2509, 12.12.2025, ELI: http://data.europa.eu/eli/reg/2025/2509/oj).

([5]) Verordening (EU) 2026/405 van het Europees Parlement en de Raad van 11 februari 2026 betreffende detergenten en oppervlakteactieve stoffen, en tot intrekking van Verordening (EG) nr. 648/2004 (PB L, 2026/405, 2.3.2026, ELI: http://data.europa.eu/eli/reg/2026/405/oj).

bij Verordening (EU) 2024/1781 ingestelde register, moeten de in deze verordening vastgestelde uitvoeringsregelingen van toepassing zijn. Hiermee mag geen afbreuk worden gedaan aan specifieke regels van de Unie betreffende het register van digitale productpaspoorten, met inbegrip van regels die zijn vastgesteld op grond van bevoegdheidsdelegaties om de vereisten ervan aan te vullen of aan te passen, zoals het geval is voor bouwproducten in artikel 79, lid 2, van Verordening (EU) 2024/3110 van het Europees Parlement en de Raad ([6]). Wanneer het register gekoppeld wordt aan andere informatiesystemen, mag die koppeling de interoperabiliteit van die systemen niet in het gedrang brengen.

(3) Om de doeltreffendheid, veiligheid en interoperabiliteit van het register te waarborgen, moet het uit de volgende componenten bestaan: een website met een beveiligde gebruikersinterface; een applicatieprogramma-interface (API) voor de registratie van digitale productpaspoorten; een verificatieplatform om het bestaan en de volledigheid van de digitale productpaspoorten te verifiëren en te bevestigen; een stelsel voor identificatie en autorisatie voor gebruikers; een stelsel voor het genereren van unieke identificatiecodes voor registratie; een component voor de opslag van de unieke identificatiecodes en goederencodes van producten waarvoor het de bedoeling is om de douaneprocedure "in het vrije verkeer brengen" te volgen; een semantisch register dat dient als gezaghebbende referentie voor de semantische betekenis, de structuur en het versiebeheer van digitale-productpaspoortgegevens en de interoperabiliteitsvereisten voor die gegevens; een logboeksysteem waarin de relevante verrichtingen worden geregistreerd. Aangezien het systeem van digitale productpaspoorten op een gedecentraliseerd model is gestoeld, moet het register ook een referentielijst bevatten van geverifieerde aanbieders van digitale-productpaspoortdiensten die in het register zijn geregistreerd.

(4) Om de verantwoordingsplicht te waarborgen, moet elke marktdeelnemer en actor in de waardeketen (zoals aanbieders van digitale-productpaspoortdiensten, reparateurs, opknapbedrijven, herproducenten, recyclers) door middel van een verificatieproces worden geïdentificeerd.

(5) In het geval van een natuurlijke persoon die als zelfstandig ondernemer optreedt die in de Unie gevestigd moet zijn, moet zijn identiteit worden aangetoond door middel van een gekwalificeerde elektronische handtekening die wordt ondersteund door een gekwalificeerd certificaat voor elektronische handtekeningen overeenkomstig Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad ([7]), of door middel van een elektronisch identificatiemiddel dat voldoet aan de eisen van die verordening met betrekking tot het betrouwbaarheidsniveau "hoog", of door middel van een krachtens de Uniewetgeving afgegeven elektronische attestering van attributen die de identificatie van de marktdeelnemer mogelijk maakt. In het geval van een natuurlijke persoon die als zelfstandig ondernemer optreedt die niet in de Unie gevestigd moet zijn, moet zijn identiteit worden aangetoond door middel van een gekwalificeerde elektronische handtekening die wordt ondersteund door een gekwalificeerd certificaat voor elektronische handtekeningen overeenkomstig Verordening (EU) nr. 910/2014, of door middel van een krachtens de Uniewetgeving afgegeven elektronische attestering van attributen die de identificatie van de marktdeelnemer mogelijk maakt.

(6) In het geval van een rechtspersoon die in de Unie gevestigd moet zijn, moet het bewijs van zijn identiteit en vestiging worden geverifieerd door een gekwalificeerde verlener van vertrouwensdiensten door middel van een gekwalificeerd elektronisch zegel dat wordt ondersteund door een gekwalificeerd certificaat voor elektronische zegels overeenkomstig Verordening (EU) nr. 910/2014, of door middel van een krachtens de Uniewetgeving afgegeven gekwalificeerde elektronische attestering van attributen die mogelijk maakt om de marktdeelnemer te identificeren en vast te stellen waar hij gevestigd is. In het geval van een rechtspersoon die niet in de Unie gevestigd hoeft te zijn, moet het bewijs van zijn identiteit en, indien van toepassing, van zijn vestiging worden geverifieerd door middel van een gekwalificeerd elektronisch zegel dat wordt ondersteund door een gekwalificeerd certificaat voor elektronische zegels dat is afgegeven door een gekwalificeerde verlener van vertrouwensdiensten overeenkomstig Verordening (EU) nr. 910/2014, of door middel van een krachtens de Uniewetgeving afgegeven elektronische attestering van attributen die de identificatie van de marktdeelnemer mogelijk maakt.

(7) Deze verordening mag geen afbreuk doen aan de vereisten in andere handelingen van de Uniewetgeving met betrekking tot de plaats van vestiging van marktdeelnemers of, in voorkomend geval, actoren in de waardeketen die producten in de handel brengen of in gebruik nemen. Daarom mag, wanneer dergelijke vereisten van toepassing zijn, het gebruik van het register de toepassing ervan niet omzeilen of ondermijnen, en moet het register worden beheerd op een wijze die volledig in overeenstemming is met die vereisten.

([6]) Verordening (EU) 2024/3110 van het Europees Parlement en de Raad van 27 november 2024 tot vaststelling van geharmoniseerde regels voor het verhandelen van bouwproducten en tot intrekking van Verordening (EU) nr. 305/2011 (PB L, 2024/3110, ELI: http://data.europa.eu/eli/reg/2024/3110/oj).

([7]) Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PB L 257 van 28.8.2014, blz. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

(8) Na voltooiing van het verificatieproces moet de marktdeelnemer worden beschouwd als een “geverifieerde marktdeelnemer”, die gemachtigd is om een gebruikersprofiel aan te maken en toegangsrechten te beheren voor extra gebruikers die namens dezelfde marktdeelnemer optreden, om nieuwe digitale productpaspoorten in het register te registreren en bestaande registraties te wijzigen. Alleen een marktdeelnemer met status “geverifieerd” mag digitale productpaspoorten in het register kunnen registreren en correcties op de bestaande registraties kunnen aanbrengen, waardoor de integriteit en nauwkeurigheid van de gegevens worden gewaarborgd. In het register moet aangegeven zijn of de registratie van de geverifieerde marktdeelnemer geldig is. Met één enkel verificatieproces moet de marktdeelnemer de status “geverifieerd” krijgen totdat zijn middel voor elektronische identificatie verstrijkt, en in ieder geval voor niet langer dan drie jaar. Wanneer een marktdeelnemer dat proces na het verstrijken van de termijn van drie jaar niet herhaalt of wanneer zijn identificatiemiddel is verstreken, mag hij niet langer als een “geverifieerde marktdeelnemer” worden beschouwd. Daarom zal hij de capaciteit verliezen om nieuwe digitale productpaspoorten te registreren of gegevens in het register te wijzigen.

(9) De actoren in de waardeketen (reparateurs, opknapbedrijven, herproducenten of andere) moeten het in artikel 5 nader beschreven verificatieproces doorlopen om toegang te krijgen tot het register. Daarom mogen alleen actoren die de status “geverifieerd” hebben verkregen, toegang hebben tot het register van digitale productpaspoorten. Hun rol (zoals reparateur, recycler, herproducent of andere) en alle handelingen die zij in het register uitvoeren, moeten worden gespecificeerd in de op grond van Verordening (EU) 2024/1781 of andere handelingen van de Uniewetgeving vastgestelde gedelegeerde handelingen.

(10) Marktdeelnemers of actoren in de waardeketen die de identiteitsverificatie niet binnen de in deze verordening vastgestelde termijn hebben doorstaan, moeten hun geregistreerde digitale productpaspoorten kunnen overdragen aan een geverifieerde marktdeelnemer of, in voorkomend geval, aan een geverifieerde actor in de waardeketen, die de verantwoordelijkheden met betrekking tot die digitale productpaspoorten moet overnemen. Die overdracht kan ook mogelijk zijn voor elke geverifieerde marktdeelnemer of geverifieerde actor in de waardeketen in geval van organisatorische veranderingen zoals fusie, splitsing of verkoop van de gehele actor of delen daarvan, beëindiging van de activiteiten of andere omstandigheden.

(11) Om de goede werking van het register en de verantwoordingsplicht van de gebruikers te waarborgen, moeten regels worden vastgesteld voor het beheer van de gegevens van gebruikersprofielen van geverifieerde marktdeelnemers en actoren in de waardeketen. Daartoe moet er voor elke geverifieerde marktdeelnemer en actor in de waardeketen altijd ten minste één aan de registerrekening verbonden persoon zijn die de profielgegevens verwerkt. Daarbij gaat het onder meer, maar niet uitsluitend, om: het, waar mogelijk, verlenen van toegangsrechten aan extra gebruikers, wijzigen en uitlezen van bestaande registraties, en registreren van nieuwe digitale productpaspoorten. Die persoon kan ook de persoon zijn die de geverifieerde marktdeelnemer of de geverifieerde actor in de waardeketen in het register registreert. De geverifieerde marktdeelnemer en de geverifieerde actor in de waardeketen moeten nauwkeurige, volledige en actuele gegevens bijhouden in het register en ervoor zorgen dat alle verstrekte informatie correct is, met inbegrip van eventuele wijzigingen betreffende hun wettelijke vertegenwoordiger. De marktdeelnemers en actoren in de waardeketen moeten ook verantwoordelijk zijn voor het beheer van het elektronisch identiteitsverificatieproces in het register. Het register mag geen belemmering vormen voor rechtmatige overdrachten van de eigendom van registraties van digitale productpaspoorten aan andere geverifieerde marktdeelnemers of actoren in de waardeketen, ongeacht hun eigen identiteitsverificatiestatus. Indien het register van digitale productpaspoorten is geïntegreerd met reeds bestaande EU-systemen (zoals het Europees productregister voor energie-etikettering (“Eprel”)) die hetzelfde verificatieniveau gebruiken voor marktdeelnemers of, in voorkomend geval, geverifieerde actoren in de waardeketen, moet dubbele verificatie worden vermeden.

(12) De bevoegde nationale autoriteiten, zoals markttoezichtautoriteiten en douaneautoriteiten, moeten voor de uitvoering van hun taken toegang hebben tot het register op grond van hun toegangsrechten zoals gespecificeerd in de relevante Uniewetgeving en de met de Uniewetgeving in overeenstemming zijnde nationale wetgeving. Om het toegangsbeheer te stroomlijnen en de verantwoordingsplicht te waarborgen, moet elke lidstaat één nationale administrateur aanwijzen als belangrijkste contactpunt met de Commissie voor het beheer van en het toezicht op de toegangsrechten voor die lidstaat. De aangewezen nationale administrateur moet optreden als de centrale autoriteit die verantwoordelijk is voor het beheer van toegangsrechten voor alle relevante nationale autoriteiten in die lidstaat, om ervoor te zorgen dat alleen bevoegde autoriteiten toegangsrechten tot het register krijgen toegewezen. De naleving van de in artikel 22 vastgestelde verplichtingen voor de lidstaat behoort niet tot de taken van de aangewezen nationale administrateurs. De lidstaten moeten de Commissie in kennis stellen van de naam en de contactgegevens van hun aangewezen nationale administrateur en van eventuele wijzigingen van deze informatie. Om de veiligheid, integriteit en vertrouwelijkheid van de gegevens te waarborgen, moet de delegatie van toegangsrechten plaatsvinden onder de volledige verantwoordelijkheid van de lidstaat, rekening houdend met de specifieke behoeften van zijn autoriteiten.

(13) De Commissie moet er bij het beheer van het register overeenkomstig artikel 13, lid 1, van Verordening (EU) 2024/1781 voor zorgen dat persoonsgegevens worden verwerkt met inachtneming van de hoogste gegevensbeschermingsnormen overeenkomstig Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([8]). De Commissie moet daarom worden beschouwd als de "verwerkingsverantwoordelijke" van het register zoals gedefinieerd in artikel 3, punt 8, van die verordening. Persoonsgegevens mogen alleen worden verwerkt ten behoeve van het beheer en de werking van het register. Die gegevens moeten worden beschermd tegen ongeoorloofde toegang, ongeoorloofd gebruik en delen zonder toestemming. Zij mogen niet langer worden bewaard dan nodig is en moeten worden gewist wanneer gebruikersaccounts worden verwijderd of de toegang wordt ingetrokken. Indien de handelingen van een gebruiker in het register echter gegevensbewaring vereisen met het oog op controle of traceerbaarheid uit hoofde van de Uniewetgeving, moeten die gegevens dienovereenkomstig worden bewaard.

(14) De registratie van het digitale productpaspoort in het register moet door de marktdeelnemer worden uitgevoerd volgens het niveau van granulariteit dat in de toepasselijke Uniewetgeving is vastgesteld, namelijk op het niveau van het model, de partij of het artikel. Om de volledige functionaliteit van het register te waarborgen, met name voor de bevoegde nationale autoriteiten en douaneautoriteiten, moeten, wanneer een digitaal productpaspoort op het niveau van het artikel wordt aangemaakt, ook de overeenkomstige identificatiecode van de partij en van het model samen met dat digitale productpaspoort in het register worden geregistreerd indien er voor het product een ontwerp van de partij en van het model bestaat. Voor producten die van nature uniek zijn, met inbegrip van handgemaakte goederen, zijn geen identificatiecodes van de partij en van het model vereist. Dezelfde regel geldt voor digitale productpaspoorten die op het niveau van de partij worden afgegeven, waarbij bij registratie een modelidentificatiecode vereist is. In dat verband moeten de identificatiecode van de partij en van het model de groepering op hoger niveau van het betrokken product weergeven. Die identificatiecodes moeten door de marktdeelnemer worden afgegeven om de bevoegde nationale autoriteiten in staat te stellen producten te traceren die tot een specifieke partij of een specifiek model behoren die of dat in het register van digitale productpaspoorten is geregistreerd. Wanneer hetzelfde product onderworpen is aan verschillende regels van de Unie op grond waarvan het digitale productpaspoort ervan op verschillende niveaus van granulariteit (model, partij of artikel) moet worden geregistreerd, moet het digitale productpaspoort op het meest granulaire niveau worden geregistreerd.

(15) Voor de registratie moet gebruik worden gemaakt van de beveiligde gebruikersinterface van het door de Commissie ter beschikking gestelde register of van de daartoe opgezette API. Zodra de registratie van een digitaal productpaspoort met succes is gevalideerd, wordt een unieke identificatiecode voor registratie gegenereerd en opgeslagen in het register en overeenkomstig artikel 8 automatisch meegedeeld aan de actor die het digitale productpaspoort registreert met behulp van dezelfde dienst die door de actor is gebruikt om de gegevens van het digitale productpaspoort te uploaden.

(16) Om ervoor te zorgen dat alleen volledige en geldige digitale productpaspoorten worden geregistreerd, moet de Commissie, als eigenaar en beheerder van het register overeenkomstig artikel 13, lid 1, van Verordening (EU) 2024/1781, een automatische verificatie van de ingediende gegevens uitvoeren. Zij moet ten minste de gegevensstructuur en het niveau van granulariteit (model, partij of artikel) van het digitale productpaspoort voor dat betrokken product verifiëren overeenkomstig de toepasselijke regels van de Unie. In voorkomend geval moeten ook de goederencodes van de producten en de link naar de door een aanbieder van digitale-productpaspoortdiensten bewaarde reservekopie, worden geverifieerd. De verificatie van de inhoudelijke juistheid van de geregistreerde gegevens blijft krachtens de toepasselijke regels van de Unie een taak van de markttoezichtautoriteiten. Bijgevolg mogen de geautomatiseerde verificaties niet worden beschouwd als bewijs van naleving van de vereisten van de op het product toepasselijke regels van de Unie, met inbegrip van de regels inzake markttoezicht.

(17) Wanneer een digitaal productpaspoort in het register is geregistreerd, heeft de marktdeelnemer, of, in voorkomend geval, een derde die namens de marktdeelnemer handelt, het recht om een bewijs van registratie op te vragen in het register. Die opvraging kan betrekking hebben op een of meer digitale productpaspoorten waarvoor de marktdeelnemer verantwoordelijk is. Het bewijs van registratie moet ten aanzien van derden als bewijs dienen dat een bepaald digitaal productpaspoort naar behoren is geregistreerd. Het moet worden aangemaakt als een beveiligd elektronisch document dat uit het register kan worden gedownload. Dat bewijs moet gedurende negentig kalenderdagen nadat het is gegenereerd beschikbaar blijven en zo nodig opnieuw kunnen worden gegenereerd.

([8]) Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(18) Om de juistheid en nauwkeurigheid van de gegevens in het register te waarborgen, moet het register het versiebeheer van geregistreerde gegevens ondersteunen. Elke nieuwe versie van het digitale productpaspoort moet aan de oorspronkelijke identificatiecode voor registratie worden gekoppeld en elke update moet van een tijdstempel worden voorzien. Met het oog op een veilige verwerking van gegevens moeten alle uitgevoerde verrichtingen ook in het register worden geregistreerd. In gevallen waarin de Uniewetgeving niet specificeert hoelang een digitaal productpaspoort beschikbaar moet blijven, zal het register de registratiegegevens van het digitale productpaspoort tien jaar na registratie automatisch verwijderen overeenkomstig de voorschriften van de mededeling van de Commissie de "Blauwe Gids" over de uitvoering van de productvoorschriften van de EU 2022 ([9]). Indien in de Uniewetgeving wel een specifieke duur is vastgesteld, worden de gegevens gedurende die specifieke duur in het register bewaard.

(19) Om de semantische interoperabiliteit van de digitale productpaspoorten en de technische werking van het register te verzekeren, moet een semantisch register worden opgezet. Het semantische register zal een evoluerende verzameling van gegevensmodellen en semantische definities zijn, die geleidelijk zal worden uitgebreid naarmate er extra productgroepen worden opgenomen. Alle gegevens in een digitaal productpaspoort moeten worden gestructureerd overeenkomstig gemeenschappelijke gegevensmodellen en semantische definities die in het semantische register van het register van digitale productpaspoorten worden gepubliceerd. Dat kader moet flexibel en uitbreidbaar blijven om toekomstige wijzigingen van de gegevensvereisten met betrekking tot de opname van een product in het digitale productpaspoort mogelijk te maken. De Commissie streeft ernaar ervoor te zorgen dat het semantische register technisch in staat is semantische specificaties te publiceren en uit te wisselen met andere registers op het niveau van de Unie, met inbegrip van die welke door de instellingen en organen van de Unie worden bijgehouden.

(20) Om het lezen, doorzoeken en vergelijken van semantische definities en gegevensstructuren mogelijk te maken, moet het semantische register een opvragingsdienst bevatten. De Commissie moet ervoor zorgen dat de inhoud van het semantische register altijd toegankelijk is via openbaar gedocumenteerde API's, behalve tijdens perioden van noodzakelijk onderhoud of tijdelijke opschorting van de dienst overeenkomstig artikel 15. De API's moeten gemeenschappelijke gegevensformaten ondersteunen om geautomatiseerd gebruik door externe systemen te vergemakkelijken. De toegang tot en het gebruik van het semantische register en de bijbehorende API's moeten kosteloos zijn.

(21) Om te zorgen voor adequate steun aan de gebruikers moet de Commissie een helpdeskdienst opzetten om waar nodig technische ondersteuning te bieden aan alle gebruikers van het register. De helpdeskdienst moet het hele jaar door tijdens de normale kantooruren operationeel zijn. Nadere bijzonderheden, waaronder operationele procedures, moeten op de website van de Commissie beschikbaar worden gesteld.

(22) Om de integriteit, veiligheid en transparantie van het register te waarborgen, moet de Commissie een robuust en geautomatiseerd logboeksysteem bijhouden waarin alle activiteiten in het register worden geregistreerd. Als onderdeel van het logboeksysteem moeten uitgebreide controlesporen worden aangemaakt. Daartoe, en om alle in het register uitgevoerde handelingen te volgen en de verantwoordingsplicht van alle gebruikers te waarborgen, moeten logboekvermeldingen betreffende zowel succesvolle als niet-succesvolle toegangspogingen, alsook wijzigingen en administratieve handelingen, worden bijgehouden.

(23) De bewaartermijnen voor de logboekvermeldingen moeten in verhouding staan tot het doel ervan. Hoewel logboekvermeldingen met betrekking tot wijzigingen van gegevens voor de duur van de registratie moeten worden bewaard ter ondersteuning van langdurige verificatie, onderzoeken van incidenten en naleving van wettelijke verplichtingen, is voor logboekvermeldingen van authenticatiepogingen een kortere bewaartermijn vereist om een evenwicht te vinden tussen de beveiligingsbehoeften en de beginselen van minimale gegevensverwerking. Logboekvermeldingen van administratieve verrichtingen en gegevensuitwisseling worden gemiddeld vijf jaar bewaard.

(24) Toegang tot logboekvermeldingen door bevoegde nationale autoriteiten en douaneautoriteiten met het oog op het uitvoeren van onderzoeken of veiligheidsaudits, of in het geval van incidenten, is van essentieel belang voor doeltreffende samenwerking en handhaving. Die toegang moet worden verleend op een wijze die de vertrouwelijkheid en integriteit van de logboekvermeldingen eerbiedigt en tegelijkertijd tijdige en grondige onderzoeken of audits mogelijk maakt.

([9]) Mededeling van de Commissie "De Blauwe Gids van 2022: richtlijnen voor de uitvoering van de productvoorschriften van de EU" (voor de EER relevante tekst), 2022/C 247/01 (PB C 247 van 29.6.2022, blz. 1).

(25) Gezien de gevoelige aard van de opgeslagen gegevens, die mogelijks persoonlijke of vertrouwelijke informatie bevatten, moet de Commissie passende technische en organisatorische maatregelen nemen om logboekvermeldingen te beschermen tegen ongeoorloofde toegang of onrechtmatige verwerking, onopzettelijk verlies of onopzettelijke vernietiging of beschadiging. Dergelijke maatregelen moeten de continuïteit en vertrouwelijkheid van de logboekvermeldingen waarborgen en ook de integriteit en betrouwbaarheid ervan als bewijs waarborgen. Het gebruik van encryptie, toegangscontroles en regelmatige integriteitscontroles moeten worden beschouwd als beste praktijken om aan deze verplichtingen te voldoen.

(26) Om het doeltreffende en efficiënte gebruik van het register te vergemakkelijken, moet de Commissie duidelijke, toegankelijke en actuele richtsnoeren en instructies over registratieprocedures en gegevensbeheer verstrekken. Het beschikbaar stellen van die hulpmiddelen via de website van de Commissie zal ervoor zorgen dat alle gebruikers, ongeacht hun technische deskundigheid, aan hun verplichtingen kunnen voldoen. Dergelijke richtsnoeren zijn van essentieel belang om fouten tot een minimum te beperken, de administratieve lasten te verminderen en een uniforme toepassing van de registratievereisten in de hele Unie te bevorderen.

(27) De voortdurende beschikbaarheid van het register is een fundamenteel vereiste voor de goede werking ervan, aangezien onderbrekingen de nalevingsactiviteiten, het markttoezicht, de douanecontroles en het vrije verkeer van goederen en diensten binnen de interne markt kunnen verstoren. Voor gepland onderhoud, zoals software-updates, beveiligingspatches of systeemupgrades, kan het echter soms tijdelijk nodig zijn om de toegankelijkheid te onderbreken. Om verstoringen te beperken, moet de Commissie dergelijke perioden vooraf meedelen op een openbaar toegankelijke website, zodat gebruikers hun plannen daarop kunnen afstemmen. Daarnaast kan de Commissie in uitzonderlijke omstandigheden, zoals systeemstoringen, cyberaanvallen of dringende veiligheidsdreigingen, de toegang tot het register zonder voorafgaande kennisgeving opschorten om gegevenslekken, ongeoorloofde toegang of verdere schade te voorkomen. Dergelijke maatregelen worden gerechtvaardigd door de dwingende noodzaak om de integriteit en de beveiliging van het register en de daarin opgenomen gegevens te beschermen. In geval van een dergelijke opschorting moet de Commissie snel handelen om de normale werking te herstellen en, waar mogelijk, de gebruikers zo spoedig mogelijk in kennis stellen van de opschorting en de verwachte duur ervan. Om de verantwoordingsplicht te waarborgen en de toegang van markttoezichtautoriteiten en douaneautoriteiten mogelijk te maken, moet de Commissie de duur en het tijdstip van eventuele onderbrekingen documenteren en die informatie ten minste vijf jaar bewaren.

(28) Het register moet voldoen aan strenge veiligheidsnormen om de integriteit, vertrouwelijkheid en beschikbaarheid van zijn gegevens te beschermen. Daarom moet de Commissie een IT-beveiligingsplan opstellen dat betrekking heeft op cyberbeveiliging en andere IT-gerelateerde risicobeoordelingen, en technische audits en steekproefsgewijze controles uitvoeren om de naleving te verifiëren en kwetsbaarheden in kaart te brengen, om ervoor te zorgen dat het systeem bestand blijft tegen cyberdreigingen. De Commissie moet ervoor zorgen dat alle beveiligingsincidenten, met inbegrip van, maar niet beperkt tot, ongeoorloofde toegang, ongeoorloofde verwerking, datalekken en gebrekkige implementatielogica, worden geregistreerd overeenkomstig de door de Commissie toegepaste beveiligingsnormen voor informatietechnologie. Bovendien moet het register, zodra de betrokken diensten op de markt van de Unie beschikbaar komen, voldoen aan een toereikend niveau van soevereiniteit, op basis van het kader voor cloudsoevereiniteit ([10]).

(29) De Commissie moet de nodige maatregelen kunnen treffen als zij het bestaan van frauduleuze activiteiten in het register vermoedt, zoals het onrechtmatig downloaden van gegevens. Gebruikers hebben de verantwoordelijkheid om de Commissie en, in voorkomend geval, de getroffen nationale autoriteiten onmiddellijk in kennis te stellen van vermeend kwaadwillig gedrag.

(30) De verwerking van persoonsgegevens in het register is noodzakelijk uit hoofde van Verordening (EU) 2024/1781, met name met het oog op de verificatie van digitale productpaspoorten, markttoezicht en douanecontroles. Om de authenticiteit en integriteit van de gegevens te waarborgen en de rechten van de betrokkenen te beschermen, moet het register de in het register opgeslagen persoonsgegevens, zoals namen, contactgegevens en inloggegevens, verwerken overeenkomstig Verordening (EU) 2018/1725.

([10]) Kader voor cloudsoevereiniteit (https://commission.europa.eu/document/09579818-64a6-4dd5-9577-446ab6219113_en).

(31) De marktdeelnemer moet verantwoordelijk zijn voor het verstrekken van nauwkeurige en volledige informatie in het register. Gezien de potentiële risico's die verbonden zijn aan ongeoorloofde toegang tot het register, zoals wijziging van gegevens, moet de marktdeelnemer worden verplicht passende technische en organisatorische beveiligingsmaatregelen te nemen om zijn IT-systemen te beschermen, met name de inloggegevens die worden gebruikt om toegang te krijgen tot het register. De marktdeelnemer moet aansprakelijk blijven ook als een derde partij gemachtigd is om in zijn naam een digitaal productpaspoort te registreren.

(32) De Commissie, die eigenaar en beheerder van het register wordt, moet verantwoordelijk zijn voor het algemene levenscyclusbeheer van het register, met inbegrip van de ontwikkeling, de beschikbaarheid, de monitoring, het updaten, het onderhoud en de hosting ervan. Dit houdt onder meer in dat de Commissie toegang heeft tot het register. De Commissie moet ook toegang kunnen krijgen tot het register om de informatie te verkrijgen die nodig is voor de uitvoering van uit hoofde van andere wetgevingshandelingen van de EU vereiste maatregelen, onder meer met het oog op markttoezicht, consumentenbescherming en naleving van de douanewetgeving.

(33) Zij moet er ook verantwoordelijk voor blijven dat de gegevens die worden bewaard in het register veilig en overeenkomstig de Uniewetgeving, waaronder de voorschriften inzake de bescherming van gegevens, worden verwerkt.

(34) De lidstaten moeten met het register kunnen interageren om hun markttoezicht, douanecontroles en andere taken die op nationaal niveau of uit hoofde van de Uniewetgeving zijn vastgesteld, doeltreffend uit te voeren. De lidstaten moeten verantwoordelijk blijven voor de ontwikkeling, het onderhoud en de beveiliging van de nationale componenten die zij gebruiken om toegang te krijgen tot het systeem, zoals nationale registers of informatiesystemen. Om een passende bescherming van persoonsgegevens te waarborgen overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad ([11]), moeten de lidstaten worden beschouwd als verwerkingsverantwoordelijken in de zin van artikel 4, punt 7, van die verordening wanneer zij persoonsgegevens verwerken voor de in de Uniewetgeving vastgestelde doeleinden. De lidstaten hebben het recht om gegevens uit het register te verwerken overeenkomstig de Uniewetgeving.

(35) De in deze verordening vervatte maatregelen zijn in overeenstemming met het advies van het bij artikel 73 van Verordening (EU) 2024/1781 opgerichte comité,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Onderwerp en toepassingsgebied

1. In deze verordening worden uitvoeringsregelingen vastgesteld voor de werking van het overeenkomstig artikel 13 van Verordening (EU) 2024/1781 opgezette register van digitale productpaspoorten, met inbegrip van regels die van toepassing zijn op marktdeelnemers die een van de volgende producten in de handel brengen of in gebruik nemen, waarvoor het bestaan van een digitaal productpaspoort en de registratie ervan in het register vereist zijn:

a) producten die vallen onder de krachtens artikel 4 van Verordening (EU) 2024/1781 vastgestelde gedelegeerde handelingen;

b) batterijen die vallen onder artikel 77 van Verordening (EU) 2023/1542;

c) bouwproducten die vallen onder artikel 76 van Verordening (EU) 2024/3110;

d) speelgoed dat valt onder artikel 19 van Verordening (EU) 2025/2509;

e) detergenten en oppervlakteactieve stoffen voor eindgebruikers die vallen onder artikel 21 van Verordening (EU) 2026/405;

f) elk ander product dat onder de wetgeving van de Unie valt waarvoor een digitaal productpaspoort en de registratie hiervan in het bij artikel 13 van Verordening (EU) 2024/1781 ingestelde register vereist zijn.

([11]) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

2. Die uitvoeringsregelingen omvatten ook regels voor het gebruik van het register door actoren in de waardeketen, bevoegde nationale autoriteiten, douaneautoriteiten en de Commissie. De in lid 1 van dit artikel bedoelde uitvoeringsregelingen en -bepalingen hebben betrekking op:

a) het beheer van de toegang tot het register;

b) het verificatieproces waarmee marktdeelnemers en actoren in de waardeketen kunnen worden geverifieerd;

c) de technische opzet van het register, met inbegrip van het semantisch register, het logboeksysteem in verband met gegevensuitwisselingsmodellen en het beheer van softwarereleases;

d) het proces van registratie en opslag van unieke identificatiecodes;

e) het proces van registratie en opslag van de goederencodes van producten waarvoor het de bedoeling is de douaneprocedure "vrijgave voor het vrije verkeer" te volgen;

f) vereisten om, in voorkomend geval, het granulariteitsniveau van het digitale productpaspoort te registreren: model, partij, artikel;

g) statussen met betrekking tot geregistreerde digitale-productpaspoortgegevens;

h) gegevens die de traceerbaarheid van producten binnen hun relevante productgroep mogelijk maken, in alle granulariteitsniveaus zoals bedoeld in artikel 8, lid 2, die van toepassing zijn op hun digitale productpaspoort;

i) het updaten en wissen van registratiegegevens;

j) de verwerking van persoonsgegevens;

k) maatregelen om oneigenlijk of frauduleus gebruik van het register te voorkomen, op te sporen en aan te pakken;

l) technische audits;

m) het waarborgen van de beschikbaarheid van het register en de daarin opgenomen gegevens.

Artikel 2

Definities

Voor de toepassing van deze verordening wordt verstaan onder:

1) "register van digitale productpaspoorten" of "register": het informatiesysteem dat door de Commissie is opgezet en wordt onderhouden overeenkomstig artikel 13 van Verordening (EU) 2024/1781;

2) "inloggegevens": een reeks unieke identificatiecodes, zoals een gebruikersnaam en wachtwoord, waarmee een gebruiker zijn identiteit kan aantonen met het oog op zijn authenticatie in het register;

3) "authenticatietoken": een token dat informatie over succesvolle authenticatie veilig doorgeeft en wordt gebruikt om geauthenticeerde sessies of gedelegeerde toegang tussen aanvragen en het informatiesysteem voor digitale productpaspoorten aan te tonen;

4) "identiteitsverificatieproces": het proces waarbij een natuurlijke persoon of rechtspersoon het bewijs levert van zijn identiteit en, in voorkomend geval, van zijn vestiging;

5) "geverifieerde marktdeelnemer": een marktdeelnemer die het identiteitsverificatieproces in het register met succes heeft voltooid overeenkomstig artikel 4;

6) "actor in de waardeketen": een natuurlijke of rechtspersoon, die geen marktdeelnemer is, die activiteiten verricht in de waardeketen van een product waarvoor een digitaal productpaspoort en de registratie ervan in het register vereist zijn, zoals een reparateur, opknapbedrijf, herproducent of recycler;

7) "geverifieerde actor in de waardeketen": een actor in de waardeketen die het identiteitsverificatieproces in het register met succes heeft voltooid overeenkomstig artikel 5;

8) “semantisch register”: een verzameling gegevensmodellen en semantische definities die bestaat uit een gestructureerde en logische reeks op elkaar betrekking hebbende termen en de desbetreffende betekenissen daarvan, die de kernelementen van het digitale productpaspoort, de definities van namen of woordenlijsten, de gegevenselementen en de met specifieke gegevens verbonden ontologie specificeren om te zorgen voor een gemeenschappelijk begrip voor alle gebruikers en taaloverschrijdende interpretatie die wordt gebruikt voor de validering van digitale productpaspoorten en voor het koppelen van de registergegevens aan de digitale productpaspoorten;

9) “semantische interoperabiliteit”: het vermogen van informatiesystemen en de organisaties die deze ondersteunen om gegevens op zodanige wijze uit te wisselen dat de betekenis van de uitgewisselde informatie door alle partijen wederzijds wordt begrepen en ondubbelzinnig kan worden geïnterpreteerd, ongeacht de onderliggende technologie of rechtsorde;

10) “gecontroleerde woordenlijst”: een gestructureerde en gezaghebbende reeks gestandaardiseerde termen met in definities vastgelegde betekenissen met het oog op een consistente weergave van gegevensattributen in alle digitale productpaspoorten;

11) “semantische specificatie”: elk artefact dat in de semantische databank wordt gepubliceerd, met inbegrip van ontologieën, gegevensmodellen, gecontroleerde woordenlijsten, en codelijsten, samen met de bijbehorende versiemetagegevens en herkomstinformatie;

12) “semantische conformiteit”: de mate waarin de gegevens in een digitaal productpaspoort voldoen aan de toepasselijke semantische specificatie, in die zin dat:

    a) alle uit hoofde van de krachtens artikel 4 van Verordening (EU) 2024/1781 vastgestelde gedelegeerde handelingen of uit hoofde van andere Uniewetgeving vereiste gegevenselementen aanwezig zijn;

    b) de verplichte (vereiste en gedefinieerde) en facultatieve (niet vereiste maar gedefinieerde) gegevenselementen die zijn gedefinieerd in de krachtens artikel 4 van Verordening (EU) 2024/1781 vastgestelde gedelegeerde handelingen of in andere Uniewetgeving, voldoen aan de toepasselijke vereisten, betreffende met name de structuur, het formaat, het waardetype, de gecontroleerde woordenlijst en regels inzake toepasbaarheid, en

    c) die gegevenselementen door andere systemen consistent kunnen worden geïnterpreteerd door verwijzing naar het toepasselijke semantische register;

13) “gegevensmodel”: een gestructureerd kader dat gegevenselementen organiseert, de structuur standaardiseert, bepaalt hoe zij zich tot elkaar verhouden en de entiteiten, hun attributen en de relatie tussen die entiteiten identificeert;

14) “logboeksysteem”: een geautomatiseerd systeem dat informatie over alle in het register uitgevoerde verrichtingen en interacties registreert en opslaat;

15) “gegevensuitwisselingsmodel”: een gestructureerd kader waarbinnen gegevens tussen verschillende systemen en platforms kunnen worden uitgewisseld;

16) “hash van de versie van het digitale productpaspoort”: de output die wordt gegenereerd uit de relevante elektronische gegevens met behulp van een bij de relevante versie van het digitale productpaspoort behorend cryptografisch algoritme;

17) “grootschalige gegevensdownload”: het opvragen van een uitzonderlijk grote of complexe gegevensverzameling — doorgaans variërend van terabyte tot petabyte in omvang — die de verwerkings- of opslagcapaciteit van conventionele instrumenten of één lokale machine overschrijdt of de waarborgen inzake monitoring verstoort.

De definities van “product”, “productgroep”, “digitaal productpaspoort”, “aanbieder van digitale-productpaspoortdiensten”, “in de handel brengen”, “ingebruikneming” en “marktdeelnemer” van respectievelijk de punten 1, 5, 28, 32, 40, 41 en 46 van artikel 2 van Verordening (EU) 2024/1781 zijn van toepassing.

Voor de toepassing van deze verordening omvat “digitaal productpaspoort” het batterijpaspoort dat is vastgesteld bij artikel 77 van Verordening (EU) 2023/1542.

De definities van “authenticatie”, “gekwalificeerde elektronische handtekening”, “gekwalificeerde verlener van vertrouwensdiensten”, “gekwalificeerd elektronisch zegel”, “gekwalificeerd certificaat voor elektronische zegels” en “elektronisch tijdstempel” van respectievelijk de punten 5, 12, 20, 27, 30 en 33 van artikel 3 van Verordening (EU) nr. 910/2014 zijn van toepassing.

De definitie van "machinaal leesbaar formaat" van punt 13 van artikel 2 van Richtlijn (EU) 2019/1024 van het Europees Parlement en de Raad ([12]) is van toepassing.

De definitie van "verwerking" van punt 3 van artikel 3 van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([13]) is van toepassing.

De definitie van "incident" van punt 6 van artikel 6 van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad ([14]) is van toepassing.

De definitie van "verwerkingsverantwoordelijke" van punt 8 van artikel 3 van Verordening (EU) 2018/1725 is van toepassing.

De definities van "markttoezicht", "markttoezichtautoriteit" en "in het vrije verkeer brengen" van respectievelijk de punten 3, 4 en 25 van artikel 3 van Verordening (EU) 2019/1020 van het Europees Parlement en de Raad ([15]) zijn van toepassing.

De definities van "douaneautoriteiten" en "douanecontroles", van respectievelijk de punten 1 en 3 van artikel 5 van Verordening (EU) nr. 952/2013 zijn van toepassing.

Artikel 3

Structuur van het register

Het register bestaat uit de volgende componenten:

a) een website met een beveiligde gebruikersinterface waarmee marktdeelnemers, actoren in de waardeketen, bevoegde nationale autoriteiten en douaneautoriteiten toegang krijgen tot het register;

b) een API voor het registreren van het digitale productpaspoort en het ontvangen van informatie uit het register;

c) een verificatieplatform om het bestaan en de volledigheid van de digitale productpaspoorten te bevestigen en te verifiëren;

d) een stelsel voor het genereren van unieke identificatiecodes voor registratie;

e) een component voor de opslag van ten minste de unieke identificatiecodes en de goederencodes voor producten waarvoor het de bedoeling is de douaneprocedure "in het vrije verkeer brengen" te volgen;

f) een lijst van de in het register geregistreerde geverifieerde aanbieders van digitale-productpaspoortdiensten;

g) een semantisch register;

h) een logboeksysteem;

i) stelsels voor identificatie en autorisatie voor gebruikers van het register.

([12]) Richtlijn (EU) 2019/1024 van het Europees Parlement en de Raad van 20 juni 2019 inzake open data en het hergebruik van overheidsinformatie (PB L 172 van 26.6.2019, blz. 56, ELI: http://data.europa.eu/eli/dir/2019/1024/oj).

([13]) Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (Voor de EER relevante tekst) (PB L 295 van 21.11.2018, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([14]) Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn) (PB L 333 van 27.12.2022, blz. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([15]) Verordening (EU) 2019/1020 van het Europees Parlement en de Raad van 20 juni 2019 betreffende markttoezicht en conformiteit van producten en tot wijziging van Richtlijn 2004/42/EG en de Verordeningen (EG) nr. 765/2008 en (EU) nr. 305/2011 (PB L 169 van 25.6.2019, blz. 1, ELI: http://data.europa.eu/eli/reg/2019/1020/oj).

Artikel 4

Verificatievereisten voor marktdeelnemers

1. Marktdeelnemers die natuurlijke personen zijn die als zelfstandig ondernemer optreden, worden als "geverifieerde marktdeelnemers" aangemerkt indien aan een van de volgende voorwaarden is voldaan:

a) indien zij in de Unie moeten gevestigd zijn, leveren zij bewijs van hun identiteit door middel van een gekwalificeerde elektronische handtekening die wordt ondersteund door een gekwalificeerd certificaat voor elektronische handtekeningen overeenkomstig Verordening (EU) nr. 910/2014, of leveren zij bewijs van hun identiteit door middel van een elektronisch identificatiemiddel dat voldoet aan de vereisten van Verordening (EU) nr. 910/2014 met betrekking tot het betrouwbaarheidsniveau "hoog", of een krachtens de Uniewetgeving afgegeven elektronische attestering van attributen die de identificatie van de marktdeelnemer mogelijk maakt;

b) indien zij niet in de Unie moeten gevestigd zijn, leveren zij bewijs van hun identiteit door middel van een gekwalificeerd elektronische handtekening die wordt ondersteund door een gekwalificeerd certificaat voor elektronische handtekeningen overeenkomstig Verordening (EU) nr. 910/2014, of van een krachtens de Uniewetgeving afgegeven gekwalificeerde elektronische attestering van attributen die de identificatie van de marktdeelnemer mogelijk maakt.

2. Marktdeelnemers die als natuurlijke personen optreden, worden als "geverifieerde marktdeelnemers" aangemerkt indien aan een van de volgende voorwaarden is voldaan:

a) indien zij in de Unie moeten gevestigd zijn, leveren zij bewijs van hun identiteit en hun vestiging door middel van een gekwalificeerd elektronisch zegel dat wordt ondersteund door een gekwalificeerd certificaat voor elektronische zegels dat is afgegeven door een gekwalificeerde verlener van vertrouwensdiensten overeenkomstig Verordening (EU) nr. 910/2014, of nadat zij bewijs van hun identiteit en van hun vestiging hebben geleverd door middel van een krachtens de Uniewetgeving afgegeven gekwalificeerde elektronische attestering van attributen die de identificatie van de marktdeelnemer mogelijk maakt;

b) indien zij niet in de Unie moeten gevestigd zijn, leveren zij bewijs van hun identiteit en, indien van toepassing, van hun vestiging door middel van een gekwalificeerd elektronisch zegel dat wordt ondersteund door een gekwalificeerd certificaat voor elektronische zegels dat is afgegeven door een gekwalificeerde verlener van vertrouwensdiensten overeenkomstig Verordening (EU) nr. 910/2014, of door middel van een krachtens de Uniewetgeving afgegeven elektronische attestering van attributen die de identificatie van de marktdeelnemer mogelijk maakt.

3. Onverminderd andere Uniewetgeving wordt toegang tot het register van digitale productpaspoorten verleend aan geverifieerde marktdeelnemers met het oog op de registratie van digitale productpaspoorten.

4. Marktdeelnemers behouden de status van geverifieerde marktdeelnemer totdat hun elektronisch identificatiemiddel verstrijkt, maar niet langer dan drie jaar na de datum van verificatie overeenkomstig lid 1 of lid 2. Zodra dergelijke middelen verstrijken of de periode van drie jaar is verstreken, naargelang wat zich het eerst voordoet, mogen marktdeelnemers niet langer nieuwe digitale productpaspoorten in het register kunnen registreren of in artikel 8 bedoelde gegevens kunnen wijzigen. Dit mogen zij alleen als zij opnieuw het identiteitsverificatieproces met succes doorlopen overeenkomstig lid 1 of lid 2. De status van het digitale productpaspoort in het register wordt dienovereenkomstig geüpdatet.

5. Onverminderd lid 4 hoeft de reeds in dat informatiesysteem geregistreerde marktdeelnemer, indien het register van digitale productpaspoorten is geïntegreerd met een ander informatiesysteem van de Unie met een gelijkwaardig of identiek identiteitsverificatieproces, geen nieuw identiteitsverificatieproces in het register van digitale productpaspoorten te ondergaan.

Artikel 5

Verificatievereisten voor actoren in de waardeketen

1. Een actor in de waardeketen die een natuurlijke persoon is die als zelfstandig ondernemer optreedt, verkrijgt een geverifieerde status in het register indien aan een van de twee volgende voorwaarden is voldaan:

a) indien zij in de Unie moeten gevestigd zijn, leveren zij bewijs van hun identiteit door middel van een gekwalificeerde elektronische handtekening die wordt ondersteund door een gekwalificeerd certificaat voor elektronische handtekeningen overeenkomstig Verordening (EU) nr. 910/2014, of leveren zij bewijs van hun identiteit door middel van een elektronisch identificatiemiddel dat voldoet aan de vereisten van Verordening (EU) nr. 910/2014 met betrekking tot het betrouwbaarheidsniveau "hoog", of een krachtens de Uniewetgeving afgegeven elektronische attestering van attributen die de identificatie van de actor in de waardeketen mogelijk maakt;

b) indien zij niet in de Unie moeten gevestigd zijn, leveren zij bewijs van hun identiteit door middel van een gekwalificeerde elektronische handtekening die wordt ondersteund door een gekwalificeerd certificaat voor elektronische handtekeningen overeenkomstig Verordening (EU) nr. 910/2014, of door middel van een krachtens de Uniewetgeving afgegeven gekwalificeerde elektronische attestering van attributen die de identificatie van de actor in de waardeketen mogelijk maakt.

2. Een actor in de waardeketen die als natuurlijke persoon optreedt, verkrijgt de status "geverifieerd" in het register indien aan een van de volgende voorwaarden is voldaan:

a) indien zij in de Unie moeten gevestigd zijn, leveren zij bewijs van hun identiteit en hun vestiging door middel van een gekwalificeerd elektronisch zegel dat wordt ondersteund door een gekwalificeerd certificaat voor elektronische zegels dat is afgegeven door een gekwalificeerde verlener van vertrouwensdiensten overeenkomstig Verordening (EU) nr. 910/2014, of leveren zij bewijs van hun identiteit en van hun vaststelling door middel van een krachtens de Uniewetgeving afgegeven gekwalificeerde elektronische attestering van attributen die de identificatie van de actor in de waardeketen mogelijk maakt;

b) indien zij niet in de Unie moeten gevestigd zijn, leveren zij bewijs van hun identiteit en, indien van toepassing, van hun vestiging door middel van een gekwalificeerd elektronisch zegel dat wordt ondersteund door een gekwalificeerd certificaat voor elektronische zegels dat is afgegeven door een gekwalificeerde verlener van vertrouwensdiensten overeenkomstig Verordening (EU) nr. 910/2014, of door middel van een krachtens de Uniewetgeving afgegeven elektronische attestering van attributen die de identificatie van de actor in de waardeketen mogelijk maakt.

3. Alleen geverifieerde actoren in de waardeketen hebben toegang tot het register en kunnen, indien dit is gespecificeerd in de desbetreffende Uniewetgeving, handelingen in het register uitvoeren.

4. Een actor in de waardeketen behoudt de status van geverifieerde marktdeelnemer totdat zijn elektronische identificatiemiddel verstrijkt, maar in ieder geval niet langer dan drie jaar na de datum van verificatie overeenkomstig lid 1 of lid 2. Zodra dergelijke middelen verstrijken of de periode van drie jaar is verstreken, naargelang wat zich het eerst voordoet, mogen deze actoren geen registraties meer kunnen uitvoeren of gegevens in het register kunnen wijzigen. Dit mogen zij alleen als zij opnieuw het identiteitsverificatieproces met succes doorlopen overeenkomstig lid 1 of lid 2.

5. Onverminderd lid 4 hoeft de reeds in dat informatiesysteem geregistreerde actor in de waardeketen, indien het register van digitale productpaspoorten is geïntegreerd met een ander informatiesysteem van de Unie met een gelijkwaardig of identiek identiteitsverificatieproces, geen nieuw identiteitsverificatieproces in het register van digitale productpaspoorten te ondergaan.

Artikel 6

Beheer van het gebruikersprofiel van de geverifieerde marktdeelnemers en geverifieerde actoren in de waardeketen

1. Indien de Uniewetgeving daarin voorziet, kunnen geverifieerde marktdeelnemers en geverifieerde actoren in de waardeketen toegangsrechten delegeren aan derde gebruikers die namens hen optreden.

2. Alle persoonsgegevens die worden ingevoerd als onderdeel van het gebruikersprofiel van een geverifieerde marktdeelnemer of geverifieerde actor in de waardeketen worden verwerkt overeenkomstig Verordening (EU) 2018/1725.

3. Elke marktdeelnemer en actor in de waardeketen is verantwoordelijk voor het beheer van zijn elektronisch verificatieproces overeenkomstig respectievelijk artikel 4 en artikel 5.

4. De geverifieerde marktdeelnemer en geverifieerde actor in de waardeketen zijn verantwoordelijk voor het updaten van hun gegevens in geval van relevante wijzigingen.

Artikel 6 bis

Overdracht van geregistreerde digitale productpaspoorten

Geregistreerde digitale productpaspoorten kunnen worden overgedragen aan een andere geverifieerde marktdeelnemer of, in voorkomend geval, aan een geverifieerde actor in de waardeketen die de verplichtingen met betrekking tot die digitale productpaspoorten van de vorige actor overneemt vanaf de voor de overdracht vermelde datum.

Artikel 7

Nationale autoriteiten

1. Uiterlijk op 18 februari 2027 wijzen de lidstaten een nationale administrateur aan die optreedt als het enig officieel contactpunt voor de Commissie voor het beheer van de toegangsrechten tot het register voor die lidstaat.

2. De lidstaten delen de Commissie de naam en de contactgegevens van hun respectieve aangewezen nationale administrateur mee en stellen de Commissie in kennis van alle latere wijzigingen met betrekking tot hun aangewezen nationale administrateur.

3. De aangewezen nationale administrateur kan toegangsrechten tot het register delegeren aan relevante nationale autoriteiten in zijn lidstaat. Een dergelijke delegatie wordt uitgevoerd onder de volledige verantwoordelijkheid van de lidstaat op een wijze die de beveiliging, integriteit en vertrouwelijkheid waarborgt van de registergegevens waartoe overeenkomstig deze verordening toegang wordt verkregen.

4. Nationale autoriteiten waaraan door hun aangewezen nationale administrateur toegang is verleend, kunnen de toegangsrechten tot het register verder delegeren en beheren binnen hun respectieve bevoegdheid.

5. Persoonsgegevens in de gebruikersprofielen en gebruikersaccounts van de bevoegde nationale autoriteiten en douaneautoriteiten worden verwerkt door de Commissie in haar hoedanigheid van verwerkingsverantwoordelijke overeenkomstig Verordening (EU) 2018/1725.

Artikel 8

Registratie van een digitaal productpaspoort

1. Voor de in artikel 1, lid 1, punt a), bedoelde producten wordt een digitaal productpaspoort geregistreerd door een geverifieerde marktdeelnemer die het product in de handel brengt of in gebruik neemt op het niveau (model, partij of artikel) dat is gespecificeerd in de toepasselijke krachtens artikel 4 van Verordening (EU) 2024/1781 vastgestelde gedelegeerde handelingen.

2. Voor de in artikel 1, lid 1, punten b) tot en met f), bedoelde producten wordt door de betrokken actor een digitaal productpaspoort geregistreerd op het in de desbetreffende Uniewetgeving gespecificeerde niveau (model, partij of artikel).

Wanneer de Uniewetgeving bepaalt dat een derde namens de in de eerste of tweede alinea bedoelde actoren handelingen in het register mag uitvoeren, mag die derde, na geverifieerd te zijn overeenkomstig artikel 19, lid 4, registratiehandelingen in het register uitvoeren.

3. Indien hetzelfde product onderworpen is aan verschillende regels van de Unie op grond waarvan de registratie van zijn digitale productpaspoort op verschillende niveaus van granulariteit (model, partij of artikel) is vereist, wordt het digitale productpaspoort voor dat product op het door de desbetreffende Uniewetgeving vereiste meest granulaire van die niveaus geregistreerd.

4. Indien het digitale productpaspoort overeenkomstig lid 1 op het niveau van een artikel wordt aangemaakt, worden de identificatiecodes voor zowel de partij als het model aan dat digitale productpaspoort gekoppeld mits er voor het product een partij- en een modelontwerp bestaan.

5. Indien het digitale productpaspoort overeenkomstig lid 1 op het niveau van een partij wordt aangemaakt, wordt de identificatiecode voor het model aan dat digitale productpaspoort gekoppeld mits er voor het product een modelontwerp bestaat.

6. De in lid 1 bedoelde relevante actor registreert een digitaal productpaspoort hetzij via de in artikel 3, punt a), bedoelde beveiligde gebruikersinterface van het register, hetzij via de in artikel 3, punt b), bedoelde API.

7. Bij indiening voor registratie leest de Commissie de inhoud van het digitale productpaspoort en verifieert zij automatisch:

a) de semantische conformiteit van de in het digitale productpaspoort verstrekte gegevens, zoals bepaald in de toepasselijke krachtens artikel 4 van Verordening (EU) 2024/1781 vastgestelde gedelegeerde handelingen of in de toepasselijke krachtens artikel 77 van Verordening (EU) 2023/1542 vastgestelde gedelegeerde handelingen, of in andere Uniewetgeving die bepaalt dat de gegevens over het digitale productpaspoort in het register van digitale productpaspoorten moeten worden geregistreerd;

b) in voorkomend geval, de samenhang tussen de verplichte gegevens die in het register moeten worden geüpload en de waarde van de gegevens die in het digitale productpaspoort worden verstrekt;

c) de conformiteit van het digitale productpaspoort met het granulariteitsniveau (model, partij of artikel), zoals bepaald in de toepasselijke uit hoofde van artikel 4 van Verordening (EU) 2024/1781 vastgestelde gedelegeerde handelingen of in de toepasselijke uit hoofde van artikel 77 van Verordening (EU) 2023/1542 vastgestelde gedelegeerde handelingen, of in andere Uniewetgeving die voorziet in een specifiek niveau voor het digitale productpaspoort dat in het register moet worden geregistreerd;

d) in voorkomend geval, de geldigheid van de goederencode van het product ten opzichte van de toegestane bandbreedtes voor deze productgroep;

e) in voorkomend geval, de link naar de door een aanbieder van digitale-productpaspoortdiensten bewaarde reservekopie.

8. Na een succesvolle verificatie overeenkomstig lid 6 genereert en bewaart het register een unieke en permanente identificatiecode voor registratie als onderdeel van de registratiegegevens.

9. Daarnaast slaat de Commissie in het register de volgende informatie op als onderdeel van de registratiegegevens:

a) in voorkomend geval, de unieke identificatiecodes;

b) in voorkomend geval, de goederencode van het product;

c) in voorkomend geval, een verwijzing naar de aanbieder van digitale-productpaspoortdiensten;

d) informatie over de registrant, met inbegrip van de datum en het tijdstip van de registratie en de integriteit van het digitale productpaspoort als onderdeel van het bewijs van de registratiegebeurtenis.

10. Wanneer de in lid 1 bedoelde relevante actor de gegevens in het register met succes indient, deelt de Commissie die marktdeelnemer automatisch de overeenkomstig lid 9 gegenereerde unieke identificatiecode voor registratie voor dat specifieke product mee. De unieke identificatiecode voor registratie wordt meegedeeld via de gebruikersinterface of het API-antwoord, naargelang de dienst die de marktdeelnemer bij de registratie gebruikt.

Artikel 9

Bewijs van registratie

1. Een marktdeelnemer of in voorkomend geval een derde partij namens de marktdeelnemer, die overeenkomstig artikel 8 een digitaal productpaspoort in het register heeft geregistreerd, moet te allen tijde een bewijs van registratie kunnen genereren voor een of meer digitale productpaspoorten waarvoor die marktdeelnemer verantwoordelijk is.

2. Het bewijs van registratie dient als bewijs, ook ten aanzien van derden, dat aan de registratieverplichting voor dat digitale productpaspoort is voldaan. Het wordt gegenereerd als een beveiligd elektronisch document dat kan worden gedownload uit het register door de actor die het digitale productpaspoort heeft geregistreerd, en het bevat ten minste de volgende gegevens:

a) de unieke productidentificatiecode;

b) in voorkomend geval, de in artikel 8, lid 9, punt b), bedoelde goederencode;

c) de naam en identiteit van de in artikel 8, lid 9, punt d), bedoelde geverifieerde marktdeelnemer die verantwoordelijk is voor de registratie;

d) de datum en het tijdstip van registratie voor de meest recente versie van het digitale productpaspoort waarvoor het bewijs is gegenereerd overeenkomstig artikel 8, lid 9, punt d), dat is gevalideerd met een elektronisch tijdstempel van de Commissie;

e) een hash van de versie van het digitale productpaspoort waarvoor het bewijs is gegenereerd.

3. Het bewijs van registratie wordt gegarandeerd door middel van een gekwalificeerd elektronisch zegel zoals bedoeld in artikel 38 van Verordening (EU) nr. 910/2014, en bevat het in lid 2, punt d), bedoelde elektronische tijdstempel van de Commissie.

4. De Commissie stelt het bewijs van registratie in het register ter beschikking van de verzoekende geverifieerde marktdeelnemer via de beveiligde gebruikersinterface van het register of via de API, naargelang de door de marktdeelnemer gekozen dienst. Dat bewijs blijft beschikbaar gedurende een periode van negentig kalenderdagen vanaf de datum waarop het is gegenereerd.

Artikel 10

Beheer van registratiegegevens

1. Elke wijziging van de gegevens voor de registratie van het digitale productpaspoort, met inbegrip van het aanmaken, wijzigen en wissen ervan, wordt overeenkomstig artikel 14 in het logboeksysteem van het register geregistreerd en weergegeven in de status van de registratie.

2. Het register ondersteunt het versiebeheer van de geregistreerde gegevens en slaat voor elke update een tijdstempel van de Commissie op.

3. Indien de Uniewetgeving niet voorziet in een specifieke duur van de beschikbaarheid van het digitale productpaspoort, worden de in artikel 8, leden 7 en 8, bedoelde registratiegegevens van het digitale productpaspoort tien jaar na de registratie automatisch uit het register verwijderd. Indien de Uniewetgeving voorziet in een specifieke duur van de beschikbaarheid van het digitale productpaspoort, wordt de bewaartermijn van dergelijke gegevens afgestemd op de duur van de beschikbaarheid van het digitale productpaspoort.

4. De gebruikers van het register hebben het recht te verzoeken om verwijdering van hun rekening indien zij niet langer verantwoordelijk zijn voor activiteiten in verband met het register.

Artikel 11

Gegevensmodellen

1. Het gegevensmodel dat van toepassing is op elke productgroep is gebaseerd op de krachtens artikel 4 van Verordening (EU) 2024/1781 vastgestelde gedelegeerde handelingen of op andere toepasselijke Uniewetgeving indien die vereisten over het betrokken gegevensmodel bevatten.

2. In voorkomend geval kunnen de gegevensmodellen voortbouwen op bestaande semantische activa, gecontroleerde woordenlijsten en referentiegegevensmodellen van de Unie.

3. Alle gegevens in een digitaal productpaspoort worden gestructureerd in overeenstemming met de gemeenschappelijke gegevensmodellen en semantische definities die in het in artikel 12 bedoelde semantische register worden gepubliceerd.

4. Gegevensmodellen moeten van een versienummer worden voorzien.

Artikel 12

Semantisch register

1. De Commissie zorgt voor het opzetten en onderhouden van een semantisch register voor digitale productpaspoorten, dat dient als gezaghebbende en machinaal leesbare bron voor de gegevensmodellen, semantische definities en woordenlijsten die van toepassing zijn op digitale productpaspoorten voor alle productgroepen. Het semantisch register wordt ontwikkeld en onderhouden overeenkomstig Verordening (EU) 2024/903 van het Europees Parlement en de Raad ([16]).

2. Het semantisch register bevat ten minste de volgende elementen:

a) de semantische betekenis van gegevensattributen die vereist zijn in een digitaal productpaspoort en technische specificaties voor het creëren, in voorkomend geval, van getypeerde en resolvabele links tussen verschillende digitale productpaspoorten, en links tussen de attributen van digitale productpaspoorten en onderliggend bewijsmateriaal dat via de productwaardeketen wordt gecommuniceerd;

b) de gegevensmodellen voor de verschillende producten binnen het toepassingsgebied van deze verordening en de formaten ervan;

c) de metagegevens die zijn verzameld met betrekking tot de gegevensmodellen voor de producten;

d) de semantische betekenis van de rollen waarin is voorzien in de toepasselijke krachtens artikel 4 van Verordening (EU) 2024/1781 vastgestelde gedelegeerde handelingen of in andere Uniewetgeving die van toepassing is op producten waarvoor een digitaal productpaspoort moet worden gebruikt;

e) meertalige labels en definities voor alle verplichte gegevensattributen.

3. De in lid 2, punt c), bedoelde metagegevens moeten in overeenstemming zijn met de DCAT-AP ([17])-specificaties.

4. De Commissie zorgt ervoor dat voor alle nieuw in het semantische register ingevoerde attributen van gegevensmodellen de in lid 2, punt e), bedoelde meertalige etiketten en definities in het semantische register worden gepubliceerd.

5. Het semantische register bevat een opvragingsdienst waarmee elke gebruiker semantische definities en gegevensstructuren kan lezen, doorzoeken en opvragen.

6. De Commissie zorgt ervoor dat de inhoud van het semantische register toegankelijk is via openbaar gedocumenteerde API's. Deze API's ondersteunen gemeenschappelijke gegevensformaten en bieden machinaal leesbare semantische activa om geautomatiseerd gebruik door externe systemen te vergemakkelijken.

7. De toegang tot en het gebruik van het semantische register en de bijbehorende API's worden kosteloos verstrekt.

Artikel 13

Technische ondersteuning

1. De Commissie voorziet in een helpdeskdienst om ervoor te zorgen dat marktdeelnemers, actoren in de waardeketen, bevoegde nationale autoriteiten en douaneautoriteiten op verzoek technische ondersteuning kunnen krijgen. De helpdeskdienst werkt het hele jaar door, van 08:00 tot 20:00 uur (plaatselijke tijd Brussel). Nadere operationele details worden op de website van de Commissie beschikbaar gesteld. Daarnaast ontwikkelt de Commissie uiterlijk in februari 2029 een geautomatiseerd instrument voor technische ondersteuning, dat het hele jaar door 24 uur per dag toegankelijk is.

2. Schriftelijke uitwisselingen tussen marktdeelnemers, actoren in de waardeketen, bevoegde nationale autoriteiten of douaneautoriteiten en de helpdesk worden bewaard tot zes maanden nadat het in lid 1 bedoelde verzoek om technische ondersteuning is afgesloten, en worden op verzoek ter beschikking gesteld van de markttoezichtautoriteiten.

([16]) Verordening (EU) 2024/903 van het Europees Parlement en de Raad van 13 maart 2024 tot vaststelling van maatregelen voor een hoog niveau van interoperabiliteit van de overheidssector in de Unie (PB L, 2024/903, 22.3.2024, ELI: http://data.europa.eu/eli/reg/2024/903/oj).

([17]) Data Catalog Application Profile (https://interoperable-europe.ec.europa.eu/collection/semic-support-centre/solution/dcat-application-profile-data-portals-europe).

Artikel 14

Logboeksysteem

1. De Commissie zorgt voor het opzetten, onderhouden en beheren van een logboeksysteem. De Commissie zorgt ervoor dat in het logboeksysteem een volledig, nauwkeurig en betrouwbaar controlespoor wordt gecreëerd.

2. In het logboeksysteem registreert de Commissie gebeurtenissen met betrekking tot alle volgende categorieën handelingen:

a) gegevens met betrekking tot toegangs- en authenticatievermeldingen;

b) wijzigingen van gegevens door alle gebruikers van het register, met inbegrip van het uploaden of bijwerken van gegevens zoals bedoeld in artikel 13, lid 4, van Verordening (EU) 2024/1781 of van gegevens die in het register moeten worden geüpload op grond van andere Uniewetgeving die het gebruik van het digitale productpaspoort voor een product verplicht stelt;

c) administratieve handelingen door alle gebruikers van het register, met inbegrip van het aanmaken, wijzigen of verwijderen van gebruikersaccounts, wijzigingen van toegangsrechten en toelatingen, en alle wijzigingen in de configuratie van het register en andere administratieve handelingen van gebruikers van het register;

d) logbestanden betreffende gegevensuitwisseling.

3. Om ervoor te zorgen dat de in het register opgeslagen gegevens veilig en in overeenstemming met de Uniewetgeving worden verwerkt, bewaart de Commissie de logbestanden gedurende een periode van:

a) zes maanden voor de in lid 2, punt a), bedoelde categorieën handelingen;

b) vijf jaar voor de in lid 2, punten c) en d), bedoelde categorieën handelingen;

c) voor de duur van de registratie voor de gebeurtenissen die verband houden met de in lid 2, punt b), bedoelde categorieën handelingen.

4. In geval van vermoedelijke incidenten en met het oog op audits en steekproefsgewijze veiligheidscontroles door de bevoegde nationale autoriteiten en douaneautoriteiten stelt de Commissie de in lid 2 bedoelde relevante logbestanden ter beschikking van de relevante nationale autoriteiten.

5. De Commissie treft passende technische en organisatorische maatregelen om de beveiliging van alle logbestanden te waarborgen en de integriteit ervan te beschermen, met name tegen ongeoorloofde of onrechtmatige verwerking, onopzettelijk verlies, vernietiging of beschadiging. Deze maatregelen waarborgen ten minste de onveranderlijkheid en vertrouwelijkheid van de logbestanden.

Artikel 15

Onderhoud en beschikbaarheid van het register

1. De Commissie stelt op haar website richtsnoeren en instructies beschikbaar over de wijze waarop gegevens in het register moeten worden geregistreerd en beheerd.

2. Het register is te allen tijde toegankelijk, behalve tijdens noodzakelijke onderhoudsactiviteiten zoals de uitrol van nieuwe software-releases, en onverminderd lid 3. In die gevallen publiceert de Commissie vooraf op de openbare website van het register een kennisgeving met betrekking tot de ontoegankelijkheid.

3. De Commissie kan de beschikbaarheid van het register zonder voorafgaande kennisgeving opschorten wanneer dit noodzakelijk is vanwege een storing, een cyberaanval of een dwingende en dringende veiligheidsbehoefte, totdat de kwestie is opgelost.

4. Wanneer registratie wordt verhinderd door tijdelijke onbeschikbaarheid of een gebrekkige werking van het register, registreert de Commissie de datum en het tijdstip van de onbeschikbaarheid en stelt zij die informatie op verzoek gedurende ten minste vijf jaar ter beschikking van de marktdeelnemers, actoren in de waardeketen, bevoegde nationale autoriteiten en douaneautoriteiten.

Artikel 16

Beveiliging van informatiesystemen en technische audits

1. De Commissie waarborgt de beveiliging van het register en de in artikel 3 bedoelde componenten. Daartoe kan de Commissie technische audits en steekproefsgewijze controles van de componenten van het register uitvoeren.

2. Voor de toepassing van lid 1 neemt de Commissie de nodige maatregelen om:

a) ongeoorloofde toegang tot het register te voorkomen;

b) ongeoorloofde verwerking van gegevens van het register te voorkomen;

c) ongeoorloofde handelingen tot het register op te sporen;

d) gegevenslekken in het register te voorkomen;

e) ervoor te zorgen dat beveiligingsincidenten worden geregistreerd overeenkomstig de door de Commissie toegepaste beveiligingsnormen voor informatietechnologie.

Artikel 17

Ongepast of frauduleus gebruik van het register

Wanneer de Commissie een ongepaste of frauduleuze activiteit in het register vaststelt, met inbegrip van een dergelijke activiteit in verband met grootschalige gegevensdownload, neemt zij de nodige maatregelen om die activiteit te voorkomen en tegen te gaan en de gevolgen ervan te beperken.

Elke gebruiker die kennis krijgt van kwaadwillige activiteiten in of tegen het register of redelijke gronden heeft om dergelijke activiteiten te vermoeden, stelt de Commissie en, in voorkomend geval, de betrokken lidstaten daarvan onmiddellijk in kennis.

Artikel 18

Persoonsgegevens

1. De Commissie slaat de volgende persoonsgegevens op in het register om de verificatie van de identiteit van alle gebruikers te waarborgen:

a) de voor- en achternaam van elke gebruiker, of, in voorkomend geval, de voor- en achternaam van de persoon die wettelijk bevoegd is om op te treden als wettelijke vertegenwoordiger van de marktdeelnemer;

b) authenticatiegegevens betreffende de gebruiker, met inbegrip van inloggegevens of authenticatietokens, die nodig zijn voor een veilige toegang tot het register;

c) het postadres van de marktdeelnemers en actoren in de waardeketen die gebruikers zijn;

d) het e-mailadres van elke gebruiker;

e) de metagegevens die zijn opgenomen in geüploade documenten indien die metagegevens bijdragen tot de identificatie of verificatie van een gebruiker.

2. In het geval van natuurlijke personen is zij ook verplicht persoonlijke identificatiemiddelen op te slaan, zoals een paspoortnummer, een nationaal identiteitskaartnummer of een nationaal eID-nummer, een burgerregistratienummer, een fiscaal identificatienummer dat is afgegeven door de relevante nationale autoriteit van de betrokken lidstaat, of een identificatiecode van een derde land die is toegekend aan een persoon of documentatie die die persoon identificeert.

3. De verzamelde persoonsgegevens worden verwerkt overeenkomstig Verordening (EU) 2018/1725.

Artikel 19

Verantwoordelijkheden van de geverifieerde marktdeelnemer

1. Een geverifieerde marktdeelnemer die een digitaal productpaspoort registreert, verstrekt aan de Commissie als beheerder van het register alle informatie die nodig is voor de registratie, zoals bepaald in artikel 8. De geverifieerde marktdeelnemer is verantwoordelijk voor de nauwkeurigheid en volledigheid van de bij de registratie ingediende informatie.

2. De geverifieerde marktdeelnemer zorgt ervoor dat de in het register van het digitale productpaspoort opgeslagen informatie te allen tijde nauwkeurig en volledig is en wordt bijgewerkt.

3. De geverifieerde marktdeelnemer is verantwoordelijk voor de uitvoering van passende technische en organisatorische beveiligingsmaatregelen voor zijn IT-systemen en inloggegevens die worden gebruikt om toegang te krijgen tot het register, om ongeoorloofde toegang tot of wijziging van registratiegegevens via zijn IT-systeem te voorkomen.

4. Wanneer een geverifieerde marktdeelnemer een derde machtigt om namens hem registratiehandelingen in het register uit te voeren, moet de derde actor het verificatieproces volgen overeenkomstig artikel 5. De geverifieerde marktdeelnemer blijft volledig verantwoordelijk voor de naleving van de in deze verordening vastgestelde verplichtingen.

5. Elke geverifieerde marktdeelnemer is verantwoordelijk voor de gegevens die hij bij de Commissie als beheerder van het register indient en wordt beschouwd als de verwerkingsverantwoordelijke van de gegevens die hij indient.

Artikel 20

Verantwoordelijkheden van de geverifieerde actoren in de waardeketen

1. Wanneer een geverifieerde actor in de waardeketen een derde machtigt om namens hem op te treden, blijft de geverifieerde actor in de waardeketen verantwoordelijk voor de naleving van de in deze verordening vastgestelde verplichtingen.

2. De geverifieerde actor in de waardeketen is verantwoordelijk voor de uitvoering van passende technische en organisatorische beveiligingsmaatregelen met betrekking tot zijn IT-systemen en inloggegevens die worden gebruikt om toegang te krijgen tot het register, om ongeoorloofde toegang tot of wijziging van registratiegegevens via zijn IT-systeem te voorkomen.

3. Wanneer de Uniewetgeving voorziet in het uploaden van informatie naar het register van digitale productpaspoorten door actoren in de waardeketen, is elke geverifieerde actor in de waardeketen verantwoordelijk voor de gegevens die hij bij de Commissie als beheerder van het register indient en wordt hij beschouwd als de verwerkingsverantwoordelijke van de gegevens die hij indient.

Artikel 21

Verantwoordelijkheden van de Commissie

1. De Commissie zorgt ervoor dat de gegevens die worden bewaard in het register veilig en overeenkomstig de Uniewetgeving, waaronder de toepasselijke voorschriften inzake de bescherming van persoonsgegevens, worden verwerkt.

2. De Commissie is de eigenaar van het register en is verantwoordelijk voor het beheer ervan, met inbegrip van de ontwikkeling, de beschikbaarheid, de monitoring, het updaten, het onderhoud en de hosting ervan.

3. De gegevens die de Commissie uit het register kan verkrijgen, kunnen worden doorgegeven aan de relevante diensten binnen de Commissie of aan de bevoegde nationale autoriteiten met het oog op de uitvoering van maatregelen die vereist zijn uit hoofde van andere wetgevingshandelingen van de EU, met name met het oog op markttoezicht, consumentenbescherming en naleving van de douanewetgeving.

Artikel 22

Verantwoordelijkheden van de lidstaten

1. Wanneer de lidstaten een koppeling met het register tot stand brengen, worden zij beschouwd als de respectieve eigenaars van hun informatiesystemen, met inbegrip van alle componenten die de lidstaten voor de koppeling hebben ontwikkeld. De lidstaten zijn verantwoordelijk voor het opzetten, de ontwikkeling, de beschikbaarheid, de monitoring, het updaten, het onderhoud en de hosting van de componenten die worden gebruikt om onder hun verantwoordelijkheid toegang te krijgen tot het register.

2. De lidstaten zorgen voor een passend beveiligingsniveau van de nationale componenten die worden gebruikt om toegang te krijgen tot het register, in overeenstemming met de Uniewetgeving. De lidstaten stellen de Commissie onverwijld in kennis van wijzigingen en updates van de componenten die onder hun verantwoordelijkheid vallen die mogelijk van invloed zijn op de werking, beschikbaarheid en betrouwbaarheid van het register.

3. De lidstaten kunnen uit het register verkregen gegevens verwerken. Wanneer de lidstaten uit het register verkregen gegevens verwerken, worden die gegevens verwerkt overeenkomstig de Uniewetgeving.

4. Bij de verwerking van persoonsgegevens met het oog op de uitvoering van hun taken uit hoofde van de Uniewetgeving of nationale wetgeving die in overeenstemming is met de Uniewetgeving, worden de lidstaten beschouwd als verwerkingsverantwoordelijken in de zin van artikel 4, punt 7, van Verordening (EU) 2016/679.

5. De lidstaten zijn verantwoordelijk voor alle gegevensverwerkingsactiviteiten die plaatsvinden binnen hun controlesfeer, met inbegrip van:

a) het beheren van de registratie en onboarding van bevoegde nationale autoriteiten en, in voorkomend geval, douaneautoriteiten, via de aangewezen nationale administrateur zoals bedoeld in artikel 7, lid 2;

b) maatregelen om ervoor te zorgen dat elke gegevensverwerking die binnen hun controlesfeer plaatsvindt, wordt uitgevoerd overeenkomstig Verordening (EU) 2016/679;

c) het intrekken van de toegangsrechten van een gebruiker tot het register in geval van ongeoorloofde of onjuiste toegang tot het register.

Artikel 23

Monitoring en evaluatie

In het kader van de monitoring en evaluatie van Verordening (EU) 2024/1781 en van de bijdrage ervan aan de werking van de interne markt voert de Commissie uiterlijk eind 2032, en vervolgens om de zes jaar, een evaluatie van deze verordening uit om rekening te houden met de werking van het register van digitale productpaspoorten, en zij dient in voorkomend geval een ontwerpvoorstel tot herziening in.

Artikel 24

Inwerkingtreding

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 16 juli 2026.

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN