ÜRÜN GÜVENLİĞİ/DPP SİCİLİ UYGULAMA TÜZÜĞÜ TASLAĞI - KAMU İSTİŞARE SÜRECİ

OSBÜK'ün tarafımıza ilettiği, T.C. Ticaret Bakanlığı Uluslararası Anlaşmalar ve Avrupa Birliği Genel Müdürlüğü'nün yazısından alınan metin, aşağıda yer almaktadır.

TİCARET BAKANLIĞI – ÜGDGM
Dijital Ürün Pasaportu – Bilgi Notu

Malumları olduğu üzere, 1/95 sayılı Ortaklık Konseyi Kararı (OKK) ile Türkiye ve Avrupa Birliği (AB) arasında oluşturulan Gümrük Birliği ile ülkemiz ürünlerin serbest dolaşımına doğrudan etki eden teknik mevzuata ilişkin AB düzenlemelerini iç hukukuna aktarmayı taahhüt etmiş olup bahse konu OKK'dan bu yana devam eden uyumlaştırma sürecinde AB teknik mevzuatındaki gelişmeler teknik mevzuat uyumundan sorumlu olan Genel Müdürlüğümüzce yakından takip edilmektedir.

Bu bakımdan, Avrupa Yeşil Mutabakatı çerçevesinde, Döngüsel Ekonomi Eylem Planı'nın bir parçası olarak Avrupa Birliği'nde yayımlanan "Sürdürülebilir Ürünler için Çevreye Duyarlı Eko-Tasarım Gereklilikleri Tüzüğü (ESPR)" ülkemizin uyumlaştırmakla yükümlü olduğu teknik bir düzenleme ve Tüzükte ürünlerin piyasaya arz koşulu olarak belirlenen Dijital Ürün Pasaportu (DPP) da bu düzenlemenin uygulanması için elzem olan yatay bir mekanizma olarak gündemimizde yer almaktadır. DPP aynı zamanda AB ekonomisinin dijitalleştirilmesine yönelik Komisyon stratejisinin de önemli bir çıktısı olarak görülmektedir. Dijital Ürün Pasaportu'nu, ürünlerin sürdürülebilirlik ve döngüsellik özellikleri ile teknik düzenlemelere uyumlarına dair bilgilere dijital olarak kolaylaştırılmış erişim sağlayan dijital bir kimlik olarak tanımlamak mümkündür. DPP, merkezi olmayan bir veri saklama yaklaşımı üzerine bina edilmektedir. Veriye erişim bir veri taşıyıcısının içine gömülü olan "tek ve benzersiz ürün tanımlayıcısı" (unique product identifier) marifetiyle, veri taşıyıcısının okutulması sonucunda erişilecek ve birer kopyası hizmet sağlayıcılar (service provider) tarafından saklanacak pasaportlara erişim ile mümkün kılınacaktır. DPP internet portalı (web portal) ise tüketiciler, iktisadi işletmeciler, geri dönüşüm ve tamir hizmeti sağlayanlar; ayrıca ülkelerin yetkili kuruluşları tarafından yetkilerine özel olarak tanımlanacak erişim hakları (access rights) temelinde ürünlerin dijital pasaportlarında yer alan verilere erişimi temin edecektir. Bu anlamda, halihazırda Enerji Etiketlemesine ilişkin Avrupa Ürün Sicilinde (EPREL) olduğu gibi tüketicilerin erişebileceği halka açık bir sayfa ile piyasa gözetimi ve denetiminden sorumlu yetkililerin erişebileceği bir bölüm bulunacaktır.

DPP'nin tasarımı iki temel üzerine inşa edilmiş bulunmaktadır. Bunlar, ürün grupları özelinde yayımlanacak mevzuatla belirlenecek ve DPP'de hangi bilgilerin yer alacağını düzenleyen "DPP verileri" (DPP-data) ile tüm ürün grupları ve mevzuatlar için yatay düzeyde geçerli olacak ve esasen işlerliği sağlayacak "DPP sistemi" (DPP-system) olarak açıklanabilir.

Bu kapsamda, DPP'de yer alacak veriler ürün gruplarına göre farklılık gösterecek olmakla birlikte ürüne ilişkin kullanım kılavuzu, etiketler, uygunluk sertifikaları, teknik performans, çevresel sürdürülebilirlik performansı, tamir edilebilirlik gibi bilgilerin DPP ile sunulması beklenmektedir.

DPP sisteminin ise, kontrol ve denetimi Avrupa Komisyonu'nda olacak olan DPP Sicili (DPP Registry) ve DPP internet portalından (web portal) oluşması beklenmektedir. DPP Sicili'nin emtia kodu (commodity code), tek ve benzersiz ürün tanımlayıcısı (unique product identifier), tek ve benzersiz işletmeci tanımlayıcısı (unique operator identifier), tek ve benzersiz tesis tanımlayıcısı (unique facility identifier) ile kayıt yapan iktisadi işletmeciye gümrük otoritelerine sunması için verilen tek ve benzersiz kayıt tanımlayıcısı (unique registration identifier - URI) bilgilerini içermesi beklenirken1;

internet portalının ise, yukarıda arz olunduğu üzere, ilgililerin (tüketici, piyasa gözetimi ve denetimi kuruluşu gibi) farklı erişim hakları doğrultusunda, mevcut DPP'lerin görüntülenmesi ve diğer DPP'lerle karşılaştırma imkanı tanıması planlanmakta olup internet portalı gerekliliklerine ilişkin ikincil yasal düzenlemelerin zaman içerisinde netlik kazanacağı anlaşılmaktadır2.

Bu kapsamda, DPP sisteminde kayıt işlemini iktisadi işletmecilerin kendilerinin gerçekleştirmesi beklenmekte; kayıt sisteminin otomatik olarak iktisadi işletmecinin başvurusu üzerine oluşturacağı URI numarasının ise üye ülkelerin gümrük otoriteleri ve DPP sistemi arasında kurulacak bağlantı sayesinde gümrük yetkililerince kontrol edilebileceği anlaşılmaktadır. Söz konusu bağlantının AB Gümrük Tek Pencere Sertifika Değişim Sistemi (EU Customs Single Window Certificates Exchange System (EU CWS-CERTEX) ile sağlanması öngörülmektedir. Bu sistemle üye ülke gümrük yetkilileri DPP Sicilinde yer alan verilere ulaşabilecek ve kontrol bu şekilde sağlanacaktır. Sistem bu şekilde risk değerlendirmesi için de kullanılabilecek, ayrıca PGD yetkilileri ile gümrük yetkililerinin de uyumsuzluk şüphesinde EU CWS-CERTEX üzerinden birlikte çalışabilecektir.

Nihai haliyle DPP'nin, iktisadi işletmeciler için artırılmış tedarik zinciri şeffaflığı, teknik gerekliliklere uyumluluğun basitleştirilmesi ve yeni iş modellerine erişim kolaylığı sağlaması; tüketiciler için bilinçli satın alımı ve ürün bilgilerine duyulan güveni artırması; düzenleyici kurumlar için ise gelişmiş piyasa gözetimi, denetimi ve yaptırımların iyileştirilmesi gibi kolaylıklar sağlaması beklenmektedir.

DPP'nin temel dayanağı ESPR olmakla birlikte halihazırda AB'de yürürlükte bulunan farklı mevzuatlarda da3 dijital ürün pasaportuna ilişkin hükümler bulunmaktadır. Söz konusu mevzuatlar arasında bulunan batarya ve yapı malzemelerine dair düzenlemeler Çevre, Şehircilik ve İklim Değişikliği Bakanlığınca, ESPR mevzuatını uyumlaştıran ülkemiz taslağı ise Sanayi ve Teknoloji Bakanlığınca hazırlanmıştır.

Öte yandan, Komisyon özellikle birlikte çalışabilirliği (interoperability) temin etmek amacıyla, DPP sisteminde yer almaya uygun mevcut standartları (GS1, ISO vb.) kullanmayı planlamakta ve bunun ötesinde ihtiyaç duyulan sekiz yeni alanda uyumlaştırılmış Avrupa standartları belirlemek üzere CEN/CENELEC bünyesinde JTC24 Ortak Teknik Komitesi ve alt komiteleri ile çalışmalarını yürütmektedir.

Yeni standart çalışmaları tek ve benzersiz tanımlayıcılar (unique identifiers); veri taşıyıcılar (data carriers) ve fiziksel ürün ile dijital temsili arasındaki bağlantılar; erişim hakları yönetimi (access rights management), bilgi güvenliği ve ticari sırlar; birlikte çalışabilirlik (interoperability), veri işleme, veri değişimi protokolleri ve veri formatları (data processing, data exchange protocols and data formats), veri depolama ve arşivleme (data storage and archiving), veri doğrulama, veri güvenilirliği ve bütünlüğü (data authentication, reliability,integrity), yaşam döngüsü yönetimi için uygulama programlama ara yüzleri (APIs for lifecycle management) konu başlıkları altında yürütülmektedir. JTC24'ün, söz konusu konu başlıklarındaki çalışmalarını tamamlaması için öngörülen süre 2025 yılı sonu olarak öngörülmekle birlikte, 2026 yılı Haziran ayı itibariyle söz konusu standartların yayımlanması; 2028 yılı itibariyle ise tüm çalışmaların tamamlaması planlanmıştır4. Bununla birlikte,

TSE'nin CEN/CENELEC'in tam üyesi olması münasebetiyle kapsamlı DPP standardizasyon çalışmalarının gerçekleştirildiği JTC24 toplantılarına katılım sağlamaya hakkı bulunmakta olup; TSE tarafından bu çalışmalar kapsamında oluşturulan ayna komiteye Genel Müdürlüğümüzce de katılım sağlanmaktadır.

Öte yandan, ESPR'da öngörüldüğü üzere söz konusu standardizasyon çalışmaları ile paralel olarak Komisyon tarafından uygulamaya yönelik ikincil mevzuat oluşturulması çalışmaları da sürdürülmektedir. Bu kapsamda, DPP verisinin işlenmesi ve depolanması yükümlülüklerini kendileri yapmayacak olan iktisadi işletmecilere bu hizmetleri sunması öngörülen hizmet sağlayıcılarının (service provider) izlemesi gerekecek kural ve gerekliliklere ilişkin olarak Avrupa Komisyonunca yetki devrine dayanan tüzük (delegated act) çalışmaları devam etmekte olup mezkûr tüzük çalışması ile birlikte bir standardizasyon çağrısı yapılmıştır. Bu kapsamda, ülkemizde faaliyet gösterecek olan hizmet sağlayıcıların talep eden iktisadi işletmeciler için hazırlayacakları DPP'lerin ilave bir doğrulama sürecine tabi olmadan AB'de kabul edilmesinin sağlanması önem arz eden bir husus olarak ön plana çıkmaktadır.

JTC24 Ortak Teknik Komitesi tarafından başlatılan standart çalışmalarının tamamlanması ile birlikte Komisyon tarafından 2026 yılı ortasına kadar hizmet sağlayıcılara ilişkin bir yetki devrine dayanan tüzük (delegated act); iktisadi işletmecilerin ve diğer aktörlerin dijital kimlik bilgilerinin düzenlenmesi ve doğrulanmasına ilişkin prosedürleri belirleyen bir uygulama tüzüğü (implementing act); AB merkezi DPP sicili (DPP Registry) için bir uygulama tüzüğü ile veri taşıyıcılar ve tek ve benzersiz tanımlayıcıların yaşam döngüsünün yönetimine ilişkin prosedür ve kuralları düzenleyen bir yetki devrine dayanan tüzük (delegated act) kabul edilmesi planlanmaktadır.

Yukarıda arz olunduğu üzere, ESPR uyumlaştırma çalışmalarımız kapsamında ülkemiz taslak mevzuatının; AB mevzuatı ile birebir uyum sağlayacak olmasından dolayı, Komisyondan alınması beklenen uyum teyidini takiben, 1/95 sayılı OKK'nın 9. Maddesi kapsamında AB üyesi ülkelerle eşit şartlar altında ülkemize DPP sisteminin iki temel aracı olan DPP siciline ve internet portalına doğrudan erişim hakkı tanınması gerektiği değerlendirilmektedir. Malumları olduğu üzere, 2/97 sayılı OKK'nın 1 sayılı Eki'nin 7. Başlığında Türkiye'nin mevzuat uyumlaştırmasının etkileri açıklanırken ilgili mevzuatta "AB üyesi ülkelere, bunların kamu veya özel kuruluşlarına veya kişilere birbirleri ile ilgili olarak tanınan haklar veya getirilen yükümlülükler, Türkiye (gerektiğinde yetkili mercileri, kamu veya özel kuruluşları veya kişileri) için de geçerli olacak şekilde anlaşılacaktır." ifadesi kullanılmaktadır.

Bu durumda DPP'lerin oluşturulmasına ve depolanmasına ilişkin hizmetleri sunacak olan ülkemizde yerleşik hizmet sağlayıcıların (service providers) da AB'deki hizmet sağlayıcılar ile aynı kategoride değerlendirilmesi ve ilave sertifikalandırmaya gerek duymadan DPP hizmeti sağlayabilmesi mümkün olabilecektir. Mevcut taslak yönetmelik, ayrıca yine DPP unsurunu içeren batarya ve atık bataryalar ile yapı malzemelerine dair taslak yönetmelikler de bu senaryo dahilinde hazırlanmış olup, DPP bölümlerinin yürürlüğe girmesi ilgili mevzuatlarda ülkemizin AB'nin DPP sistemine erişim sağlamasına paralel olacak şekilde kurgulanmıştır.

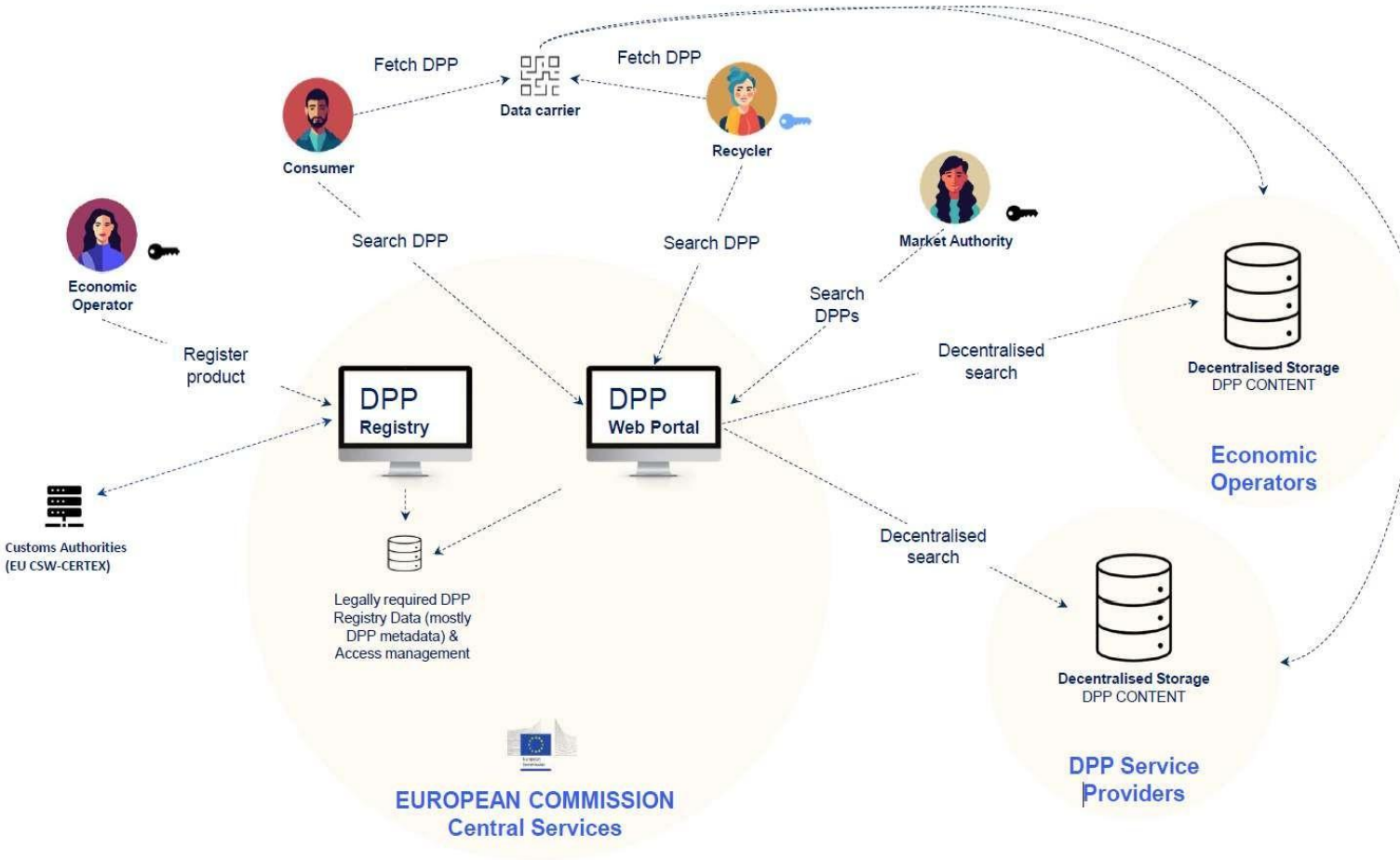
Bu kurgu içinde Bakanlığımızın yukarıda arz edilen DPP sisteminin altyapısını teşkil edecek yatay mevzuatı hazırlamaktan sorumlu olmasının uygun olacağı; öte yandan, ürün bazlı DPP düzenlemelerinin yayımlanmasından ilgili yetkili kuruluşların sorumlu olmasının gerektiği değerlendirilmektedir.

Bununla birlikte, bu husus, ESPR mevzuatının birebir uyumlu hale getirilmesinin yanı sıra AB ile hâlihazırda süregelen yeni tip mevzuat kapsamında yer alan ve örnekleri EPREL ve RAPEX veri tabanlarında da görülen yatay mekanizmalara ülkemizin erişimine dair müzakerelerin sonuçlarına (ve bu anlamda kişisel verilerin korunması, ticari sır ve Elektronik Kimlik ve Hizmet Güvenilirliği Yönetmeliği (e-IDAS) mevzuatımızın AB tarafından kabulüne) bağlı bulunmaktadır.

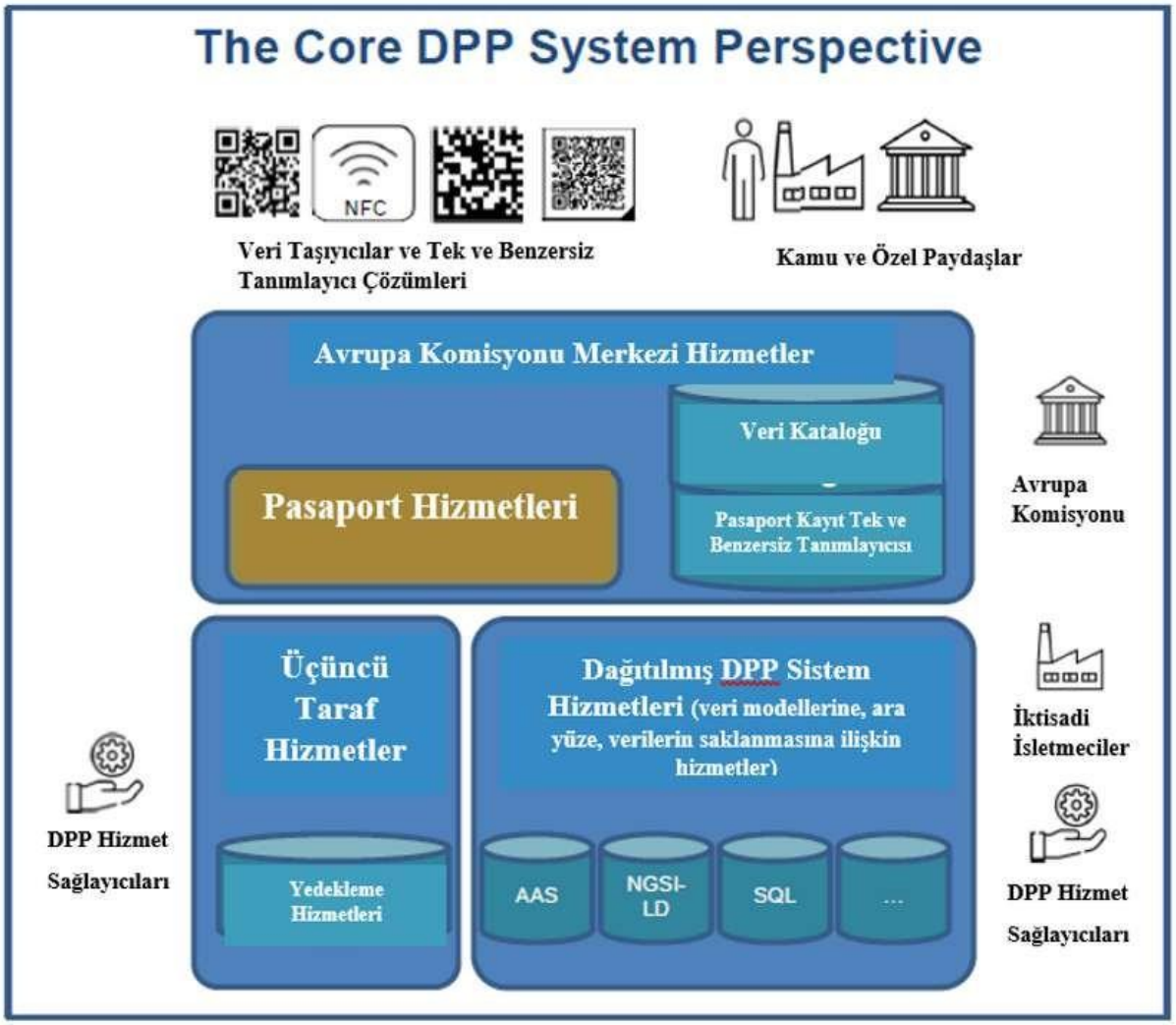
Öte yandan, Türkiye'nin DPP veri tabanına ve internet portalına erişememesi halinde ülkemizin kendi DPP sistemini oluşturması gerekecektir.

TİCARET BAKANLIĞI – ÜGDGM
Dijital Ürün Pasaportu – Bilgi Notu

EK-1



EK-3


The Core DPP System Perspective
NFC
Veri Taşıyıcılar ve Tek ve Benzersiz Tanımlayıcı Çözümleri
Kamu ve Özel Paydaşlar
Avrupa Komisyonu Merkezi Hizmetler
Veri Kataloğu
Pasaport Hizmetleri
Pasaport Kayıt Tek ve Benzersiz Tanımlayıcısı
Avrupa Komisyonu
Üçüncü Taraf Hizmetler
Dağıtılmış DPP Sistem Hizmetleri (veri modellerine, ara yüze, verilerin saklanmasına ilişkin hizmetler)
İktisadi İsletmeciler
DPP Hizmet Sağlayıcıları
Yedekleme Hizmetleri
AAS
NGSI-LD
SQL
...
DPP Hizmet Sağlayıcıları

EK-4

Sektörel Mevzuat Bakımından DPP		
Yönetmelik	**Durum**	**DPP Uygulaması**
Batarya ve Atık Batarya Yönetmeliği	Yürürlükte	QR kod aracılığıyla Batarya Pasaportu
Yapı Malzemeleri Yönetmeliği	Yürürlükte	Yapı Malzemeleri Dijital Ürün Pasaportu Sistemi
Ambalaj ve Atık Ambalajı Yönetmeliği	Yürürlükte	Uyumlaştırılmış etiket sistemi
Oyuncak Güvenliği	Teklif aşamasında	Uyumluluk bilgisi, uygunluk beyanı, CE işaretlemesi
Deterjanlar	Teklif aşamasında	Uygulama yasaları ile zorunlu olan teknik gereklilikler

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of XXX

laying down the implementation arrangements for the digital product passport registry set up under Regulation (EU) 2024/1781 of the European Parliament and of the Council

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024 establishing a framework for the setting of ecodesign requirements for sustainable products, amending Directive (EU) 2020/1828 and Regulation (EU) 2023/1542 and repealing Directive 2009/125/EC[1], and in particular Article 13(5), second subparagraph, in conjunction with Article 13(5), third subparagraph, thereof,

Whereas:

(1) Article 13(1) of Regulation (EU) 2024/1781 requires the Commission to establish a digital registry for the digital product passport ('the registry') to store in a secure manner at least the unique identifiers. It is necessary to set out the main components of the registry and lay down the technical and operational roles and obligations of economic operators placing a product on the market or putting it into service within the framework of the digital product passport registry, competent national authorities and customs authorities, and the Commission. Furthermore, it is necessary to establish a log system in order to record and monitor the operations and interactions carried out in the registry in order to ensure accountability for all users, and delineate the responsibility for the maintenance, operation and security of the registry.

(2) The registry should provide information about products covered by delegated acts adopted under Regulation (EU) 2024/1781 and, about batteries, under Regulation (EU) 2023/1542 of the European Parliament and of the Council[2]. Other Union legislation may require that information on products be stored in the registry. That is already the case for construction products within the scope of Regulation (EU) 2024/3110 of the European Parliament and of the Council[3], toys falling within the scope of Regulation (EU) 2025/2509 of the European Parliament and of the Council[4] and detergents falling

[1] OJ L, 2024/1781, 28.6.2024, p.1, ELI: http://data.europa.eu/eli/reg/2024/1781/oj.

[2] Regulation (EU) 2023/1542 of the European Parliament and of the Council of 12 July 2023 concerning batteries and waste batteries, amending Directive 2008/98/EC and Regulation (EU) 2019/1020 and repealing Directive 2006/66/EC (OJ L 191, 28.7.2023, p. 1, ELI: http://data.europa.eu/eli/reg/2023/1542/oj).

[3] Regulation (EU) 2024/3110 of the European Parliament and of the Council of 27 November 2024 laying down harmonised rules for the marketing of construction products and repealing Regulation (EU) No 305/2011 (OJ L, 2024/3110, 18.12.2024, ELI: http://data.europa.eu/eli/reg/2024/3110/oj).

[4] Regulation (EU) 2025/2509 of the European Parliament and of the Council of 26 November 2025 on the safety of toys and repealing Directive 2009/48/EC (OJ L, 2025/2509, 12.12.2025, ELI: http://data.europa.eu/eli/reg/2025/2509/oj).

within the scope of Regulation (EU) 2026/405 of the European Parliament and of the Council[5]. Where other Union legislation refers to the registry established by Regulation (EU) 2024/1781, the implementation arrangements laid down in this Regulation should apply.

(3) To ensure the effectiveness, security and interoperability of the registry, it should consist of the following elements: a website providing a secure user interface; an Application Programming Interface (API) for registering digital product passports; a verification platform to verify all users; an identification and authorisation scheme for users; a schema for generating unique registration identifiers; a storage of the commodity codes of products intended to be placed under the customs procedure 'release for free circulation'; a semantic repository which serves as the authoritative reference for the semantic meaning, structure, versioning and interoperability requirements of digital product passport data; a log system recording relevant operations. Considering that the digital product passport system is built on a decentralised model, the registry should also include a reference list of digital product passport service providers which host backup copies of digital product passports.

(4) In order to ensure that necessary data is uploaded and unique identifiers are stored in the registry, each economic operator should be identified by a verification process. That verification process should be carried out also by any other actor in the value chain (such as digital product passport service providers, authorised representatives, repairers, refurbishers, remanufacturers, recyclers), who updates the data of a product's digital product passport.

(5) In the case of a natural person acting as a sole trader who is established in the Union, identity should be proved through a qualified electronic signature supported by a qualified certificate for electronic signatures in accordance with Regulation (EU) No 910/2014 of the European Parliament and of the Council[6], or through an electronic identification means which meets the requirements of that Regulation with regard to the assurance level 'high', or through an electronic attestation of attributes issued under Union law that enables the identification of the economic operator. In the case of a natural person acting as a sole trader who is not established in the Union, identity should be proved through a qualified electronic signature supported by a qualified certificate for electronic signatures in accordance with Regulation (EU) No 910/2014, or through an electronic attestation of attributes issued under Union law that enables the identification of the economic operator.

(6) In the case of a legal person established in the Union, proof of identity and where applicable, of establishment should be verified by a qualified trust service provider through a qualified electronic seal supported by a qualified certificate for electronic seals in accordance with Regulation (EU) No 910/2014, or through a qualified electronic attestation of attributes issued under Union law that enables the identification of the economic operator. In the case of a legal person not established in the Union, proof of identity and where applicable, of establishment should be verified

---

5 Regulation (EU) 2026/405 of the European Parliament and of the Council of 11 February 2026 on detergents and surfactants, and repealing Regulation (EC) No 648/2004 (OJ L, 2026/405, 2.3.2026, ELI: http://data.europa.eu/eli/reg/2026/405/oj).

6 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

by means of a qualified electronic seal supported by a qualified certificate for electronic seals, issued by a qualified trust service provider pursuant to Regulation (EU) No 910/2014, or by means of an electronic attestation of attributes issued under Union law that enables the identification of the economic operator.

(7) Upon completion of the verification process, the economic operator should be considered a 'verified economic operator', authorised to create a user profile and manage access rights to additional users acting on behalf of the same operator, to register new digital product passports in the registry and modify existing registrations. Only a verified economic operator should be able to register digital product passports in the registry and make corrections to the existing ones, thereby ensuring the integrity and accuracy of the data. The registry will use statuses to indicate whether the registration of the verified economic operator is valid. A single verification process should provide the economic operator with the 'verified' status up until their means for electronic identification expire but no longer than for 3 years. After that period, a new verification process should be performed. If the economic operator does not seek renewal (repeat the verification process according to Article 4) the economic operator should be considered an 'unverified economic operator' and lose the capacity to register new digital product passports and upload any data in the registry. In cases of insolvency, liquidation or cessation of activity in the Union of the verified economic operator responsible for the creation of the digital product passport, the record of the digital product passport shall remain available in the registry for the period specified in the relevant Union law.

(8) In order for other value chain actors (repairers, refurbishers, remanufacturers or other) to get access to the registry or to update information in a digital product passport, those actors will need to go through a verification process, detailed in Article 5. Therefore, only actors who obtained the status 'verified' shall have access to the digital product passport registry. Their role (such as repairer, recycler, remanufacturer or other) and any actions which they perform in the registry should be specified in the delegated acts adopted under Regulation (EU) 2024/1781 or under other Union law.

(9) In order to ensure proper functioning of the registry and accountability for users, rules should be laid down for managing the user profile data of verified economic operators and other verified value chain actors. For that purpose, a verified economic operator and a verified value chain actor should always have at least one person linked to the registry account who handles the profile data, which includes but is not limited to, granting access rights to additional users where practicable, modifying and reading existing registrations, and registering new digital product passports. It can also be the same person who registers the verified economic operator or the verified value chain actor in the registry. The verified economic operator and the verified value chain actor should maintain accurate, complete, up-to-date records and ensure all information provided is correct, including any changes to its legal representative. The economic operator and other value chain actors should also be responsible for managing the electronic identity verification process in the registry. Where the digital product passport registry is integrated with already established EU systems, such as the European Product Registry for Energy Labelling ('EPREL'), that use the same level of verification for economic operators or, where relevant, for other verified value chain actors, double verification will be avoided.

(10) Competent national authorities and customs authorities should have access to the registry for the purposes of carrying out their duties based on their access rights specified in relevant Union and national laws in compliance with Union law. In order

to streamline access management and ensure accountability, each Member State should designate a single national administrator as the main contact point with the Commission to manage and oversee access rights for their Member State. The designated national administrator should act as the central authority responsible for managing access rights for all relevant national authorities within that Member State, to ensure that only relevant authorities are assigned access rights to the registry. Member States should inform the Commission of their appointed national administrator's name and contact details and notify the Commission of any changes to this information. In order to ensure the security, integrity and confidentiality of the data, the delegation of access rights should be carried out under the full responsibility of the Member State taking into account the specific needs of its authorities.

(11) The Commission, in managing the registry in accordance with Article 13(1) of Regulation (EU) 2024/1781, should ensure that personal data is processed in accordance with the highest data protection standards in accordance with Regulation (EU) 2018/1725 of the European Parliament and of the Council[7]. The Commission should therefore be considered the registry's 'controller' as defined in Article 3, point (8), of that Regulation. Personal data should only be collected and used for managing access to the registry. That information should be protected from unauthorised access, use, or sharing. That data should only be kept as long as necessary and should be deleted when user accounts are removed or access is revoked. However, if a user's actions in the registry require data retention for auditing or traceability under Union law, that data should be kept accordingly.

(12) Registration of the digital product passport in the registry should be carried out by the economic operator at least at the level of granularity set out in the applicable Union law (model, batch or item level). In order to ensure full functionality of the registry, in particular for competent national authorities and customs authorities, where a digital product passport is created on item level, both the batch and model identifiers should be registered together with that digital product passport in the registry, provided that batch and model design exist for the product. For unique products, such as handmade goods, no batch and model identifiers are required. The same rule applies for digital product passports issued at batch level, where a model identifier is required upon registration.

(13) Registration should be carried out by using the secure user interface of the registry provided by the Commission or through the API set up for that purpose. Once the registration of a digital product passport is successfully validated, a unique registration identifier is generated and stored in the registry and communicated according to Article 8 automatically to the actor registering the digital product passport using the same service which was used by the actor to upload the digital product passport data.

(14) To ensure that only complete and valid digital product passports are registered, the Commission should, as the owner and manager of the registry in accordance with Article 13(1) of Regulation (EU) 2024/1781, perform an automatic verification of the submitted data. Such verification should confirm at least the existence and semantic completeness of mandatory data, the conformity of the digital product passport to the

[7] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

level of granularity (model, batch or item) as required under relevant Union law, and the use of a valid qualified electronic signature or seal, in accordance with the standards set out in Regulation (EU) No 910/2014. Where relevant, the product commodity codes and the link to the back-up hosted by a digital product passport service provider should also be subject to verification.

(15) Where a digital product passport is registered in the registry, the economic operator is entitled to request proof of registration from the registry. That request can cover one or more digital product passports for which the economic operator is responsible. The proof of registration should serve as evidence for third parties that a particular digital product passport has been properly registered. It should be created as a secure electronic document, which can be downloaded from the registry. That proof should remain available for 90 calendar days from the date of its generation, with the possibility of regeneration, if necessary.

(16) To ensure the correctness and accuracy of registry data, the registry should support versioning of registered data. Each new version of the digital product passport should be linked to the original registration identifier, and each update should be time- stamped. For the purpose of secure handling of data, all operations performed should also be logged in the registry. In cases where Union law does not specify how long a digital product passport must remain available, the registry will automatically delete the digital product passport registration data 10 years after registration in accordance with the rules laid down in Commission notice The 'Blue Guide' on the implementation of EU product rules 2022[8]. Where Union law does set a specific duration, the data will be kept in the registry for that specific period.

(17) To ensure semantic interoperability and technical functioning of the registry, a semantic repository should be set up. The semantic repository will be an evolving collection of data models and semantic definitions, expanding progressively as additional product groups are incorporated. All data contained in a digital product passport needs to be structured in accordance with common data models and semantic definitions published in the semantic repository of the registry. That framework should remain flexible and extensible to accommodate any future changes to data requirements regarding the inclusion of a product in the digital product passport. The Commission strives to ensure that the semantic repository is technically capable of publishing semantic specifications and exchanging them with other Union level repositories, including those maintained by Union institutions and bodies.

(18) To allow reading, searching and comparing of semantic definitions and data structures, the semantic repository should include a search service. The Commission should ensure that the content of the semantic repository is accessible through publicly documented APIs at all times except during periods of necessary maintenance or temporary suspension of the service in accordance with Article 15. The APIs should support common data formats to facilitate automated use by external systems. Access to and use of the semantic repository and its APIs should be free of charge.

(19) To ensure support to users, the Commission should establish a helpdesk service to provide technical support to all users of the registry where needed. The helpdesk

[8] Commission notice The 'Blue Guide' on the implementation of EU product rules 2022 (Text with EEA relevance) 2022/C 247/01 (OJ C 247, 29.6.2022, pp. 1–152).

service should be available during the Commission's working days, as determined yearly by the Commission Decision on public holidays for officials and other servants of the European Union serving in Brussels and Luxembourg, and during normal working hours. Those working days shall be published on the Commission's website.

(20) To ensure the integrity, security and transparency of the registry, the Commission should maintain a robust and automated log system recording all activities within the registry. As part of the log system, comprehensive audit trails should be created. To that end, and to track all actions performed on the registry in order to ensure accountability for all users, logs should be kept of access attempts, both successful and unsuccessful, as well as modifications and administrative actions.

(21) The retention periods for logs should be proportionate to their purposes. While logs related to modifications, administrative actions, and exchanges should be retained for the duration of the registration to support long-term verification, incident investigations, and compliance with legal obligations, logs of authentication attempts require a shorter retention period to balance security needs with data minimisation principles.

(22) Access to logs by competent national authorities and customs authorities for the purpose of conducting investigations or security audits, or in the event of incidents, is essential for effective cooperation and enforcement. Such access should be granted in a manner that respects the confidentiality and integrity of the logs, while allowing for timely and thorough investigations or audits.

(23) Given the sensitive nature of the logged data, which may include personal or confidential information, the Commission should implement appropriate technical and organisational measures to protect logs against unauthorised access or unlawful processing, accidental loss, destruction or damage. Such measures should guarantee the continuity and confidentiality of logs as well as ensure their integrity and reliability as evidence. The use of encryption, access controls, and regular integrity checks should be considered best practices to fulfil these obligations.

(24) To facilitate the effective and efficient use of the registry, the Commission should provide clear, accessible and up-to-date guidelines as well as instructions on registration procedures and data management. Making those resources available through the Commission website will ensure that all users, regardless of their technical expertise, are able to comply with their obligations. Such guidance is essential to minimise errors, reduce administrative burdens, and promote uniform application of the requirements to register across the Union.

(25) The continual availability of the registry is a fundamental requirement for its proper functioning, as interruptions could disrupt compliance activities, market surveillance, customs controls and the free movement of goods and services within the internal market. However, planned maintenance, such as software updates, security patches, or system upgrades, may occasionally necessitate temporary inaccessibility. To mitigate disruptions, the Commission should provide advance notice of such periods on a publicly accessible website, allowing users to plan accordingly. Additionally, in exceptional circumstances, such as system malfunctions, cyber-attacks, or urgent security threats, the Commission may suspend access to the registry without prior notice to prevent data breaches, unauthorised access, or further damage. Such measures are justified by the overriding need to protect the integrity and security of the registry and the data it contains. In the event of such suspension, the Commission should act swiftly to restore normal operations and, where feasible, inform users, as

soon as practicable, of the suspension and its expected duration. To ensure accountability and enable access by market surveillance authorities and customs authorities, the Commission should document the duration and timing of any outages and retain such records for at least five years.

(26) The registry should operate in compliance with high-level security standards to protect the integrity, confidentiality and availability of its data. Therefore, the Commission should prepare an IT Security Plan which will cover cybersecurity and other IT related risk assessments, conduct technical audits and random checks to verify compliance and identify vulnerabilities, which will ensure that the system remains resilient against cyber threats. The Commission should ensure that all security events, which include but are not limited to unauthorised access, unauthorised processing, data breaches, fails of implementation logic, are logged in accordance with the information technology security standards applied by the Commission. In addition, the registry should comply, as soon as the relevant services become available on the Union market, with an adequate level of sovereignty, based on the Cloud Sovereignty Framework[9].

(27) The Commission should be able to take the necessary action if it suspects fraudulent activity in the registry, which may include inappropriate downloading of information. [Users have the responsibility to notify the Commission and, whether relevant, the affected national authorities immediately in case of suspected malicious behaviour.]

(28) The processing of personal data in the registry is necessary under Regulation (EU) 2024/1781, including the verification of digital product passports, market surveillance, and customs controls. To ensure the authenticity and integrity of the data and to protect the rights of data subjects, the registry should process personal data stored in it, such as names, contact information, and login credentials, in accordance with Regulation (EU) 2018/1725.

(29) The economic operator should be responsible for providing accurate and complete information to the registry. Given the potential risks associated with unauthorised access to the registry, such as data modification, the economic operator should be obliged to implement adequate technical and organisational security measures to protect its IT systems, in particular the credentials used to access the registry. The economic operator should remain liable even if a third party is authorised to register a digital product passport on behalf of the economic operator.

(30) The Commission, which is to be the owner and manager of the registry, should be responsible for the overall lifecycle management of the registry, including its development, availability, monitoring, updating, maintenance, and hosting. That entails inter alia the fact that the Commission has access to the registry. The Commission should also be able to access the registry in order to obtain information that is necessary for carrying out measures required under other EU legislative acts, including for the purposes of market surveillance, consumer protection and customs compliance.

(31) It should also remain responsible for ensuring that the data stored in it is processed securely and in compliance with Union law, including with the data protection rules.

(32) Member States need to be able to interact with the registry to effectively carry out their market surveillance, customs controls, and other tasks laid down at national level or

[9] https://commission.europa.eu/document/09579818-64a6-4dd5-9577-446ab6219113_en

under Union law. Member States should remain responsible for ensuring the development, maintenance and security of national components which they use to access the system, such as national registries or information systems. To ensure appropriate protection of personal data, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council[10], Member States should be regarded as controllers within the meaning of Article 4, point (7), of that Regulation, when they process personal data for the purposes laid down in Union law.

(33) The measures provided for in this Regulation are in accordance with the opinion of the Committee established by Article 73 of Regulation (EU) 2024/1781,

HAS ADOPTED THIS REGULATION:

Article 1

Subject matter and scope

1. This Regulation sets out implementation arrangements for the functioning of the digital product passport registry established in accordance with Article 13 of Regulation (EU) 2024/1781 including rules which apply to economic operators that place any of the following products on the market or put them into service:

   (a) products covered by delegated acts adopted pursuant to Article 4 of Regulation (EU) 2024/1781;

   (b) batteries covered by Article 77 of Regulation (EU) 2023/1542;

   (c) construction products covered by Article 76 of Regulation (EU) 2024/3110;

   (d) toys covered by Article 19 of Regulation (EU) 2025/2509;

   (e) detergents covered by Article 21 of Regulation (EU) 2026/405;

   (f) any other product covered by Union legislation requiring a digital product passport and its registration in the registry established under Article 13 of Regulation (EU) 2024/1781.

2. The implementation arrangements and rules referred to in paragraph 1 of this Article relate to:

   (a) management of access to the registry;

   (b) the verification process that allows economic operators and other value chain actors to be verified;

   (c) the technical set-up of the registry, including semantics repository, log system related to data exchange models and software release management;

   (d) the process of registering and storing unique identifiers;

   (e) the process of registering and storing commodity codes for products intended to be placed under the customs procedure ‘release for free circulation’;

   (f) requirements to register, where relevant, product parameters: models, batches, items;

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(g) statuses related to registered digital product passport data;

(h) data that will allow the traceability of products within their relevant product group, across the granularity levels, as referred to in Article 8(2), applicable for their digital product passport;

(i) update and deletion of registration data;

(j) processing of personal data;

(k) measures aimed at preventing, detecting and addressing any improper or fraudulent use of the registry;

(l) technical audits;

(m) ensuring the availability of the registry and of the data it contains.

Article 2
Definitions

For the purposes of this Regulation, the following definitions apply:

(1) 'digital product passport registry' or 'registry' means the information system established and maintained by the Commission in accordance with Article 13 of Regulation (EU) 2024/1781;

(2) 'login credentials' means a set of unique identifiers, such as a username and password, that enables a user to verify its identity in order to authenticate themselves in the registry;

(3) 'authentication token' means a token that securely transmits information about successful authentication and is used to prove authenticated sessions or delegated access between applications and the digital product passport information system;

(4) 'identity verification process' means the process by which a natural person or legal person provides the evidence of identity and of establishment that entitles such person to register a digital product passport in the registry;

(5) 'verified economic operator' means an economic operator that has successfully completed the identity verification process in the registry in accordance with Article 4;

(6) 'unverified economic operator' means an economic operator that has not successfully completed or renewed the identity verification process in the registry in accordance with Article 4;

(7) 'semantic repository' means a collection of data models and semantic definitions that are composed of a structured and logically interrelated set of terms and their meanings specifying the core elements of the digital product passport, the definitions of names or vocabularies, the data elements and the ontology associated with specific data in order to ensure common understanding across all users, and cross-lingual interpretation used for digital product passport validation and for linking the registry data with the digital product passports;

(8) 'semantic interoperability' means the ability of information systems and the organisations that support them to exchange data in such a way that the meaning of exchanged information is mutually understood and unambiguously interpretable by all parties, regardless of the underlying technology or jurisdiction;

(9) ‘machine-readable format’ means a machine-readable format as defined in Article 2, point (13), of Directive (EU) 2019/1024 of the European Parliament and of the Council[11];

(10) ‘controlled vocabulary’ means a structured and authoritative set of standardised terms with defined meanings with a view to ensuring consistent representation of data attributes across digital product passports;

(11) ‘semantic specification’ means any artefact published in the semantic repository, including ontologies, data models, controlled vocabularies, and code lists, together with their versioning metadata and provenance information;

(12) ‘data model’ means a structured framework that organises elements of data, standardises the structure, determines how they relate to one another, and identifies the entities, their attributes and the relationship between those entities;

(13) ‘log system’ means an automated system that records and stores information on all operations and interactions carried out in the registry;

(14) ‘data exchange model’ means a structured framework through which data can be exchanged between different systems and platforms;

(15) ‘semantic conformity’ means the extent to which data for a digital product passport meets the semantic requirements laid down in Article 12;

(16) ‘hash of the version of the digital product passport’ means the output generated from the relevant electronic data using a cryptographic algorithm from the relevant version of the digital product passport.

The definition of ‘release for free circulation’ as set out in Article 3, point (25), of Regulation (EU) No 952/2013 of the European Parliament and of the Council[12] applies.

The definitions of ‘product’, ‘product group’, ‘digital product passport’, ‘digital product passport service provider’, ‘placing on the market’, ‘putting into service’, ‘economic operator’, as set out in Article 2, points (1), (5), (28), (32), (40), (41) and (46), respectively, of Regulation (EU) 2024/1781, apply.

For the purposes of this Regulation, ‘digital product passport’ includes the battery passport established by Article 77 of Regulation (EU) 2023/1542.

The definitions of ‘authentication’, ‘qualified electronic signature’, ‘qualified trust service provider’, ‘qualified electronic seal’, ‘qualified certificate for electronic seal’ and ‘electronic time stamp’, as set out in Article 3, points (5), (12), (20), (27), (30) and (33), respectively, of Regulation (EU) No 910/2014, apply.

The definition of ‘processing’, as set out in Article 3, point (2), of Regulation (EU) 2018/1807 of the European Parliament and of the Council[13], applies.

---

[11] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast) (OJ L 172, 26.6.2019, p. 56, ELI: http://data.europa.eu/eli/dir/2019/1024/oj).

[12] Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code (OJ L 269, 10.10.2013, p. 1, ELI: http://data.europa.eu/eli/reg/2013/952/oj).

[13] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (OJ L 303, 28.11.2018, p. 59, ELI: http://data.europa.eu/eli/reg/2018/1807/oj).

The definition of 'incident', as set out in Article 6, point (6), of Directive (EU) 2022/2555 of the European Parliament and of the Council[14], applies.

The definition of 'controller', as set out in Article 3, point (8), of Regulation (EU) 2018/1725, applies.

The definitions of 'market surveillance' and 'market surveillance authority', as set out in Article 3, points (3) and (4), respectively, of Regulation (EU) 2019/1020 of the European Parliament and of the Council[15], apply.

The definitions of 'customs authorities' and 'customs controls', as set out in Article 5, points (1) and (3), respectively, of Regulation (EU) No 952/2013, apply.

Article 3

Structure of the registry

The registry shall consist of the following:

(a) a website providing a secure user interface for economic operators, other value chain actors than economic operators, competent national authorities and customs authorities to access the registry;

(b) an API for registering the digital product passport and receiving information from the registry;

(c) a verification platform to confirm and verify the existence and completeness of the digital product passports;

(d) a scheme for generating unique registration identifiers;

(e) commodity codes for products intended to be placed under the customs procedure 'release for free circulation';

(f) a list of the digital product passport service providers;

(g) a semantic repository;

(h) a log system;

(i) identification and authorisation schemes for registry users.

Article 4

Verification requirements for economic operators

1. Economic operators that are natural persons acting as sole traders shall be qualified as 'verified economic operators' if one of the two following conditions is satisfied:

   (a) (in case they are established in the Union) they submit evidence of their identity by means of a qualified electronic signature supported by a qualified certificate for electronic signatures in accordance with Regulation (EU) No

[14] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

[15] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (OJ L 169, 25.6.2019, p. 1, ELI: http://data.europa.eu/eli/reg/2019/1020/oj).

910/2014; or they submit evidence of their identity by means of an electronic identification means that meets the requirements of Regulation (EU) No 910/2014 with regard to the assurance levels 'high', or an electronic attestation of attributes issued under Union law that enables the identification of the economic operator;

(b) (in case they are not established in the Union) they submit evidence of their identity by means of a qualified electronic signature supported by a qualified certificate for electronic signatures in accordance with Regulation (EU) No 910/2014, or an electronic attestation of attributes issued under Union law that enables the identification of the economic operator.

2. Economic operators acting as legal persons shall be qualified as 'verified economic operators' if one of the two following conditions is satisfied:

(a) (in case they are established in the Union) they submit evidence of their identity and, where applicable, of their establishment by means of a qualified electronic seal supported by a qualified certificate for electronic seal, issued by a qualified trust service provider pursuant to Regulation (EU) No 910/2014; or after submitting evidence of their identity by means of a qualified electronic attestation of attributes issued under Union law that enables the identification of the economic operator;

(b) (in case they are not established in the Union) they submit evidence of their identity and, where applicable, of their establishment by means of a qualified electronic seal supported by a qualified certificate for electronic seal, issued by a qualified trust service provider pursuant to Regulation (EU) No 910/2014, or an electronic attestation of attributes issued under Union law that enables the identification of the economic operator.

3. Only verified economic operators may register digital product passports in the registry. Any correction to that information shall be performed without undue delay.

4. Economic operators shall retain the status as verified economic operators until their electronic identification means expire but no longer than three years from the date of verification in accordance with paragraph 1 or 2. Once such means expire or the three-year period has expired, whichever is first, economic operators shall be able to register new digital product passports in the registry only if they successfully repeat the identity verification process in accordance with paragraph 1 or 2. The validity status of the digital product passport in the registry shall be updated accordingly.

Article 5

Verification requirements for other value chain actors

1. A value chain actor other than the economic operator who is a natural person acting as a sole trader shall obtain a verified status in the registry if one of the two following conditions is fulfilled:

(a) (in case they are established in the Union) they submit evidence of their identity by means of a qualified electronic signature supported by a qualified certificate for electronic signatures in accordance with Regulation (EU) No 910/2014; or they submit evidence of their identity by means of an electronic identification means that meets the requirements of Regulation (EU) No 910/2014 with regard to the assurance levels 'high', or an electronic attestation

of attributes issued under Union law that enables the identification of the economic operator;

(b) (in case they are not established in the Union) they submit evidence of their identity by means of a qualified electronic signature supported by a qualified certificate for electronic signatures in accordance with Regulation (EU) No 910/2014, or an electronic attestation of attributes issued under Union law that enables the identification of the economic operator.

2. A value chain actor other than the economic operator acting as a legal person shall obtain a verified status in the registry if one of the two following conditions is satisfied:

(a) (in case they are established in the Union) they submit evidence of their identity and, where applicable, of their establishment by means of a qualified electronic seal supported by a qualified certificate for electronic seal, issued by a qualified trust service provider pursuant to Regulation (EU) No 910/2014; or they submit evidence of their identity by means of a qualified electronic attestation of attributes issued under Union law that enables the identification of the economic operator;

(b) (in case they are not established in the Union) they submit evidence of their identity and, where applicable, of their establishment by means of a qualified electronic seal supported by a qualified certificate for electronic seal, issued by a qualified trust service provider pursuant to Regulation (EU) No 910/2014, or an electronic attestation of attributes issued under Union law that enables the identification of the economic operator.

3. Value chain actor other than the economic operator who has obtained verified status, shall have access to the digital product passport registry.

4. Value chain actor other than the economic operator shall retain the status as verified until their electronic identification means expire and in any event no longer than three years from the date of verification in accordance with paragraph 1 or 2. Once such means have expired or once the three-year period has expired, whichever ever is first, these actors shall be able to access the registry only if they successfully repeat the identity verification process in accordance with paragraph 1 or 2.

Article 6

Management of verified economic operator and other verified value chain actor user profile

1. Verified economic operators and other verified value chain actors may delegate access rights to users acting on their behalf. Each verified economic operator and other verified value chain actor shall be responsible for the actions carried out by a user acting on their behalf.

2. Any personal data which is entered as part of the user's profile of verified economic operator or other verified value chain actor shall be processed in accordance with Regulation (EU) 2018/1725[16].

[16] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No

3. Each economic operator and other value chain actor shall be responsible for managing their electronic verification process in accordance with Articles 4 and 5 respectively.

4. The verified economic operator and other verified value chain actor shall be responsible for ensuring that the data about itself is updated in case of any relevant change, including any change of its legal representative.

Article 7
National authorities

1. Member States shall appoint a designated national administrator who shall act as the single official contact point for the Commission for the purposes of managing registry access rights for that Member State.

2. Member States shall communicate to the Commission the name and contact details of their respective designated national administrator and shall notify the Commission of any subsequent changes with regard to their designated national administrator.

3. The designated national administrator may delegate registry access rights to relevant national authorities within its Member State. Such delegation shall be carried out under the full responsibility of the Member State and in a way that ensures the security, integrity and confidentiality of the registry data accessed in accordance with this Regulation.

4. National authorities which have been granted access by their designated national administrator may delegate and manage registry access rights further within their respective authority.

5. Personal data contained in the user profiles and user accounts of the competent national authorities and customs authorities shall be processed by the Commission in its capacity as controller in accordance with Regulation (EU) 2018/1725.

Article 8
Registration of a digital product passport

1. For products referred to in Article 1(1), point (a), a digital product passport shall be registered by economic operator placing the product on the market or putting it into service at least at the level specified in the applicable delegated acts (model, batch or item level) adopted pursuant to Article 4 of Regulation (EU) 2024/1789.

2. For products referred to in Article 1(1), points (b) to (f), a digital product passport shall be registered by the relevant actor at the level (model, batch or item level) specified in the relevant Union law.

3. Where the digital product passport is created at item level, in accordance with paragraph 1, both batch and model identifiers shall be linked to that digital product passport where batch and model design exist in the production.

4. Where the digital product passport is created at batch level, in accordance with paragraph 1, the model identifier shall be linked to that digital product passport where model design exists in the production.

45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.) OJ L 295, 21.11.2018, ELI: http://data.europa.eu/eli/reg/2018/1725/oj

5. An economic operator shall register a digital product passport either through the secure user interface of the registry as provided for in Article 3, point (a), or through the API as provided for in Article 3, point (b).

6. Upon submission for registration, the Commission shall automatically verify:

   (a) the existence and semantic conformity of mandatory data to be uploaded in the registry as provided for in the applicable delegated acts adopted pursuant to Article 4 of Regulation (EU) 2024/1781 or in the applicable delegated acts adopted pursuant to Article 77 of Regulation (EU) 2023/1542, or under other Union law providing for data to be registered in the digital product passport registry;

   (b) the conformity of the digital product passport with the granularity level (model, batch or item) as provided for in the applicable delegated acts adopted pursuant to Article 4 of Regulation (EU) 2024/1781 or in the applicable delegated acts adopted pursuant to Article 77 of Regulation (EU) 2023/1542, or under other Union law providing for a specific level for the digital product passport to be registered in the registry;

   (c) where relevant, the validity of the commodity code of the product in relation to the permitted ranges for this product group;

   (d) where relevant, the link to the back-up hosted by a digital product passport service provider;

   (e) the use of a qualified electronic signature or a qualified electronic seal in accordance with Regulation (EU) No 910/2014.

7. Following a successful verification in accordance with paragraph 4, the registry shall generate and store a unique and persistent registration identifier as part of the registration data.

8. Additionally, the Commission shall store in the registry the following information as part of the registration data:

   (a) where relevant, the unique identifiers;

   (b) where relevant, the commodity code of the product;

   (c) where relevant, reference to the digital product passport service provider;

   (d) registrant information, including date and time of the registration and the integrity of the digital product passport as part of the evidence of the registration event.

9. Upon successful submission by the relevant actor as referd to in paragraph 1, of the data in the registry, the Commission shall automatically communicate to that economic operator the unique registration identifier for that specific product generated in accordance with paragraph 5. The unique registration identifier shall be communicated through the user interface or the API response, depending on the service used by the economic operator during registration.

Article 9

Proof of registration

1. An economic operator or another relevant actor that has registered a digital product passport in the registry in accordance with Article 8 shall be able to generate, at any

given time, proof of registration for one or more digital product passports for which that economic operator is responsible.

2. The proof of registration shall serve as evidence, including vis-à-vis third parties, that the registration obligation for that digital product passport has been fulfilled. It shall be generated as a secure electronic document that can be downloaded by the actor that registered the digital product passport from the registry, containing at least the following data:

   (a) the unique and persistent registration identifier generated in accordance with Article 8(5);

   (b) the commodity code as referred to in Article 8(6), point (b);

   (c) the name and identity of the verified economic operator responsible for the registration as referred to in Article 8(6), point (d);

   (d) the date and time of the registration for the latest version of the digital product passport for which the proof is generated in accordance with Article 8(6), point (d), which is validated by an electronic time stamp of the Commission;

   (e) a hash of the version of the digital product passport for which the proof is generated.

3. Proof of registration shall be guaranteed by means of a qualified electronic seal as provided for in Article 38 of Regulation (EU) No 910/2014 and by means of a qualified timestamp as provided for in Article 42 of that Regulation.

4. The Commission shall make available in the registry to the requesting verified economic operator the proof of registration through the registry's secure user interface or through the API, depending on the service chosen by the economic operator. That proof shall remain available for a period of 90 calendar days from the date of its generation.

Article 10

Registration data management

1. Any change to the digital product passport registration data, including its creation, modification and deletion, shall be logged in the log system of the registry in accordance with Article 14 and reflected in the status of the registration.

2. The registry shall support the versioning of the registered data by linking each new digital product passport version to the original registration identifier and storing a timestamp of the Commission for each update.

3. Where Union law does not provide for a specific duration of availability of the digital product passport, digital product passport registration data, as referred to in Article 8(5) and (6), shall be deleted automatically from the registry 10 years after registration. Where Union law provides for a specific duration of availability of the digital product passport, the retention period of such data shall be aligned with the period of availability of the digital product passport.

4. Registry users have the right to request deletion of their respective account if they are no longer responsible for activities related to the registry.

Article 11

Data models

1. All data contained within a digital product passport shall be structured in accordance with the common data models and semantic definitions published in the semantic repository referred to in Article 12. Data models shall, where applicable, reuse existing EU-level semantic assets, controlled vocabularies and reference data models.

2. The data model for each product group shall provide the structure for at least the following categories of data:

   (a) data required in accordance with Regulation 2024/1781 and with the applicable delegated acts supplementing that Regulation;

   (b) data required in accordance with other Union legislation applicable to the product that mandates the use of a digital product passport for that product.

3. Data models shall be versioned.

Article 12

Semantic repository

1. The Commission shall establish and maintain a digital product passport semantic repository, which serves as an authoritative and machine-readable source for the data models, semantic definitions and vocabularies applicable to digital product passports across all product groups. The semantic repository shall be developed and maintained in accordance with Regulation (EU) 2024/903 of the European Parliament and of the Council[17].

2. The semantic repository shall lay down in particular:

   (a) the semantic meaning of data attributes required within a digital product passport and technical specifications for creating, where relevant, typed and resolvable links between different digital product passports, and links between digital product passport attributes and underlying evidence communicated through the product value chain;

   (b) the structure of the data models for the different products in scope and their formats;

   (c) the metadata collected regarding the data models for the data products;

   (d) the semantic meaning of the roles provided for in the applicable delegated acts adopted pursuant to Article 4 of Regulation (EU) 2024/1781, or by other Union legislation applicable to any product that is required to use a digital product passport;

   (e) multilingual labels and definitions for all mandatory data attributes.

3. The metadata as referred to in paragraph 2 letter (c) shall be in conformity with the DCAT-AP[18] specifications.

[17] Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (OJ L, 2024/903, 22.3.2024, ELI: http://data.europa.eu/eli/reg/2024/903/oj).

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

4. The Commission shall ensure that the multilingual coverage for the mandatory data attributes as referred to in paragraph 2 letter (d) that are new is published in the semantic repository.

5. The semantic repository shall include a search service to allow any user to read, search and retrieve semantic definitions and data structures.

6. The Commission shall ensure that the content of the semantic repository is accessible through publicly documented APIs. These APIs shall support common data formats and provide machine-readable semantic assets to facilitate automated use by external systems.

7. Access to and use of the semantic repository and its APIs shall be provided free of charge.

Article 13
Technical support

1. The Commission shall provide a helpdesk service to ensure that economic operators, other valu chain actors, competent national authorities and customs authorities are able to receive technical support upon request. The helpdesk service shall be available during the Commission's working days, as determined yearly by the Commission Decision on public holidays for officials and other servants of the European Union serving in Brussels and Luxembourg, and during normal working hours. Those working days shall be published on the Commission's website. However, technical support for urgent requests shall be ensured on working days between 27 and 31 December.

2. Written exchanges between economic operators, other valu chain actors, competent national authorities or customs authorities and the helpdesk shall be stored for six months after the request referred to in paragraph 1 has been closed and made available to market surveillance authorities upon request.

Article 14
Log system

1. The Commission shall establish, maintain and run a log system. The Commission shall ensure the creation of a complete, accurate and reliable audit trail in the log system.

2. In the log system the Commission shall log events for all of the following categories of actions:

   (a) data related to access and authentication entries;

   (b) data modifications by all registry users, including the uploading or updating of data referred to in Article 13(4) of Regulation (EU) 2024/1781 or of data required to be uploaded in the registry pursuant to other Union legislation that mandates the use of the digital product passport for a product;

   (c) administrative actions by all registry users, including the creation, change or deletion of user accounts, changes to access rights and permissions, and any changes to the registry's configuration and other administrative actions of registry users;

   (d) data exchange logs.

3. To ensure that the data stored in the registry is processed securely and in compliance with Union law, the Commission shall keep the logs for a period of:

   (a) six months for the categories of actions referred to in paragraph 2, point (a);

   (b) five years for the categories of actions referred to in paragraph 2, points (c) and (d);

   (c) for the duration of the registration for the categories of actions referred to in paragraph 2, point (b).

4. In the case of suspected incidents and for the purposes of audits and random checks of security performed by competent national authorities and customs authorities, the Commission shall make the relevant logs referred to in paragraph 2 available to the relevant national authorities.

5. The Commission shall implement appropriate technical and organisational measures to guarantee the security of all logs and protect their integrity, in particular against unauthorised or unlawful processing, accidental loss, destruction or damage. Such measures shall, at least, ensure the immutability and confidentiality of the logs.

Article 15
Maintenance and registry availability

1. The Commission shall make available on its website guidelines and instructions on how to register and manage data in the registry.

2. The registry shall be accessible at all times, except during necessary maintenance activities such as deployment of new software releases, and without prejudice to paragraph 3. In those instances, the Commission shall issue an advance notice of inaccessibility on the public website of the registry.

3. The Commission may suspend the availability of the registry, without prior notice, where it is necessary in view of a malfunction or of a cyber-attack or a compelling urgent security need, until the issue is resolved.

4. Where registration is prevented by the temporary unavailability or malfunctioning of the registry, the Commission shall record the date and time of unavailability and make such information available to economic operators, other value chain actors, competent national authorities and customs autorities upon request for no less than five years.

Article 16
Information system security and technical audits

1. The Commission shall ensure the security of the registry and its components as referred to in Article 3. To that end, the Commission may conduct technical audits and random checks on the components of the registry.

2. For the purposes of paragraph 1, the Commission shall take the necessary measures in order to:

   (a) prevent any unauthorised access to the registry;

   (b) prevent any unauthorised processing of registry data;

   (c) detect any unauthorised activities in the registry;

(d) avoid any data breaches of the registry;

(e) ensure that security events are logged in accordance with the information technology security standards applied by the Commission.

Article 17

Inappropriate or fraudulent use of the registry

Where the Commission identifies an inappropriate or fraudulent activity in the registry, including any such activity linked to massive data download, it shall take the necessary measures aiming at avoiding and countering that activity and mitigating the effects thereof.

Any user who becomes aware of, or has reasonable grounds to suspect, malicious behaviour in or against the registry shall immediately inform thereof the Commission and the Member States concerned.

Article 18

Personal data

1. The Commission shall store the following personal data in the registry to ensure the verification of the identity of all users:

   (a) first and last name of each user; or first and last name of the person legally entitled to act as a legal representative for the economic operator, where applicable;

   (b) authentication credentials associated with the user, including login credentials or authentication tokens, necessary for secure access to the registry;

   (c) postal address of the economic operators and other value chain actors that are users;

   (d) email address of each user;

   (e) metadata embedded in uploaded documents where such metadata contributes to the identification or verification of a user.

2. In the case of natural persons, it shall also be required to store personal identifiers, such as a passport number, national identity card number or national eID number, civil registry number, tax identification number issued by the relevant national authority of the respective Member State, or any third-country identifier that is assigned to a person or documentation that identifies that person.

3. Personal data collected shall be processed in accordance with Regulation (EU) 2018/1725.

Article 19

Responsibilities of the verified economic operator

1. A verified economic operator requesting the registration of a digital product passport shall provide the Commission as manager of the registry with all information necessary for the registration, as provided for in Article 8. The verified economic operator shall be responsible for the accuracy and completeness of the information submitted at the time of registration.

2. The verified economic operator shall ensure that the information stored in the registry of the digital product passport is kept accurate, complete and up to date at all times.

3. The verified economic operator shall be responsible for implementing appropriate technical and organisational security measures to its IT systems and credentials used to access the registry, to prevent any unauthorised access to or modification of registration data through its IT system.

4. Where a verified economic operator authorises a third party to perform registration actions in the registry on its behalf, the verified economic operator shall remain fully responsible for compliance with the obligations set out in this Regulation.

5. Each verified economic operator shall be responsible for the data it submits to the Commission as manager of the registry and shall be considered as the controller of the data it submits.

Article 20

Responsibilities of other verified value chain actors

1. Where a verified value chain actor other than the economic operator authorises a third party to act on its behalf, the verified value chain actor shall remain responsible for compliance with the obligations set out in this Regulation.

2. A verified value chain actor other than the economic operator shall be responsible for implementing appropriate technical and organisational security measures with regard to its IT systems and credentials that are used to access the registry, in order to prevent any unauthorised access to or modification of registration data through its IT system.

3. Where Union law provides for other value chain actors than economic operators to upload any information to the digital product passport registry, each verified value chain actor shall be responsible for the data it submits to the Commission as manager of the registry and shall be considered as the controller of the data it submits.

Article 21

Responsibilities of the Commission

1. The Commission shall ensure that the data stored in the registry is processed securely and in compliance with Union law, including applicable rules on the protection of personal data.

2. The Commission shall be the owner of the registry and responsible for its management, including its development, availability, monitoring, updating, maintenance and hosting.

3. The data that the Commission can obtain from the registry may be transmitted to the relevant services within the Commission or to competent national authorities for the purposes of carrying out measures required under other EU legislative acts, including market surveillance, consumer protection and customs compliance.

Article 22

Responsibilities of the Member States

1. Where Member States create an interconnection with the registry, they shall be considered the respective owners of their information systems, including any components developed by Member States for the interconnection. Member States shall be responsible for the establishment, the development, availability, monitoring,

updating, maintenance and hosting of the components used to access the registry under their responsibility.

2. Member States shall ensure an appropriate level of security of the national components used to access the registry, in accordance with Union law. Member States shall inform, without undue delay, the Commission of changes and updates to the components under their responsibility that may affect the functioning, availability and reliability of the registry.

3. When processing personal data for the purposes of carrying out their duties defined in Union law or under national law in compliance with Union law, Member States shall be regarded as controllers as defined in Article 4, point (7), of Regulation (EU) 2016/679.

4. Member States shall be responsible for any data processing activities, including:

   (a) managing the registration and onboarding of competent national authorities and where relevant, customs authorities, through the designated national administrator as referred to in Article 7(2);

   (b) ensuring that any data processing taking place within their sphere of control is performed in accordance with Regulation (EU) 2016/679;

   (c) withdrawing a user's rights of access to the registry in case of unauthorised or incorrect access to the registry.

Article 23

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the Commission
The President
Ursula von der Leyen