**Recital 42:** Essential and important entities should ensure the security of the network and information systems which they use in their activities. Those are primarily private network and information systems managed by their internal IT staff or the security of which has been outsourced. The cybersecurity risk management and reporting requirements pursuant to this Directive should apply to the relevant essential and important entities regardless of whether they perform the maintenance of their network and information systems internally or outsource it.

42(aa). ***Taking account of their cross-border nature, the DNS service providers, TLD name registries and entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, and managed security service providers should be subject to a higher degree of harmonisation at Union level. The implementation of cyber security measures should therefore be facilitated by an implementing act.***

**Recital 59:** Maintaining accurate and complete databases of domain names and registration data (so called ‘WHOIS data’) and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the Union. ***For this specific purpose, TLD registries and the entities providing domain name registration services should be required to process certain data necessary to achieve the purpose.*** Such processing ***should constitute a legal obligation in the meaning of A4rticle 6(1)(c) of Regulation 2016/679. This obligation is without prejudice to the possibility to collect domain name registration data for other purposes, for example based on contractual arrangements or legal requirements established in other Union or national laws***.

**Recital 60:** The availability and timely accessibility of ***the domain name registration*** data to ***legitimate access seekers, is essential to prevent and combat Domain Name System abuse, to prevent, detect and respond to cybersecurity incidents.***

***Legitimate access seekers mean any legal or natural person making a request based on Union or national law. They include but are not limited to*** competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, ***and national*** CERTs, ***or*** CSIRTs***.***

***TLD registries and the entities providing domain name registration services should be required to enable lawful access to specific domain name registration data, which are strictly necessary for the purpose of the access request, to legitimate access seekers in accordance with Union and national law.***

***The request from legitimate*** access ***seekers*** should ***be accompanied with a statement of reasons permitting the assessment of the necessity of access to the*** data.

**Recital 61:** In order to ensure the availability of accurate and complete domain name registration data, TLD registries and the entities providing domain name registration services should collect and guarantee the integrity and availability of domain names registration data. In particular, TLD registries and the entities providing domain name registration services for the TLD should establish policies and procedures to collect and maintain accurate and complete registration data, as well as to prevent and correct inaccurate registration data in accordance with Union data protection rules. ***These policies and procedures should take into account to the extent possible the standards developed by the multi-stakeholder governance structures at international level.***

***The TLD registries and the entities providing domain name registration services should adopt and implement proportionate processes to verify such registration data. These processes should reflect the current best practices used within the industry and, to the extent possible, the progress being made in the field of electronic identification. Examples of verification processes may include both ex ante controls, performed at the time of the registration, and ex post controls, performed after the registration.***

***The TLD registries and the entities providing domain name registration services should in particular verify at least one means of contact of the registrant.***

**Recital 62:** TLD registries and the entities providing domain name registration services ***should be required to make publicly*** available domain name registration data that fall outside the scope of Union data protection rules, such as data that concern legal persons***1. For legal persons, the TLD name registries and the entities providing domain name registration services should make publicly available at least the name of the registrant, and the contact telephone number. The contact email address should also be published provided that it does not contain any personal data. This can be achieved through various technical means, including the use of email aliases, functional accounts or similar systems.***

TLD registries and the entities providing domain name registration services for the TLD should also enable lawful access to specific domain name registration data concerning natural persons to legitimate access seekers, in accordance with Union data protection law. Member States should ensure that TLD registries and the entities providing domain name registration services for them should respond without undue delay to requests for the disclosure of domain name registration data ***from legitimate access seekers.***

TLD registries and the entities providing domain name registration servicesshould establish policies and procedures for the publication and disclosure of registration data, including service level agreements to deal with requests for access from legitimate access seekers. ***These policies and procedures should take into account, to the extent possible any guidance and the standards developed by the multi-stakeholder governance structures at international level.*** The access procedure may also include the use of an interface, portal or other technical tool to provide an efficient system for requesting and accessing registration data.

***Member States should ensure that all types of access to domain name registration data (both personal and non-personal data) are free of charge.***

With a view to promoting harmonised practices across the internal market, the Commission may adopt guidelines on such procedures without prejudice to the competences of the European Data Protection Board ***and take into account to the extent possible the standards developed by the multi-stakeholder governance structures at international level***.

**Recital 63:** Essential and important entities under this Directive should fall under the jurisdiction of the Member State where they ***are established. Providers of public electronic communications networks or providers of electronic communications services should be deemed to be under the jurisdiction of the Member State in which they*** provide their services. If the entity provides services ***or is established*** in more than one Member State, it should fall under the separate and concurrent jurisdiction of each of these Member States. The competent authorities of these Member States should cooperate, provide mutual assistance to each other and where appropriate, carry out joint supervisory actions. ***Where Member States exercise jurisdiction, they should avoid that the same conduct is sanctioned more than once for the infringement of the obligations laid down in this Directive, in line with the principle of ne bis in idem. DNS service providers, TLD name registries, and entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, and managed security service providers, as well as digital providers should be deemed to be under the jurisdiction of the Member State in which they have their main establishment in the Union. Public administration entities should fall under the jurisdiction of the Member State which established them.***

63(a). ***For the purpose of ensuring compliance of the entities with their obligations under this Directive, Member States should cooperate and assist each other in the performance of supervisory and enforcement measures, notably when services are provided in more than one Member State or when the network and information systems are located in a different Member State than the ones where services are provided. When providing assistance, the competent authority the assistance of which was requested should carry out supervisory or enforcement measures in accordance with its national law. In order to ensure the smooth functioning of the mutual assistance mechanism established under this Directive, competent authorities should use the Cooperation Group as a forum to discuss cases and particular requests for assistance.***

**Recital 64:** In order to take account of the cross-border nature of the services and operations of DNS service providers, TLD name registries, ***entities providing domain name registration services,*** content delivery network providers, cloud computing service providers, data centre service providers and digital providers, only one Member State should have jurisdiction over these entities. Jurisdiction should be attributed to the Member State in which the respective entity has its main establishment in the Union. The criterion of establishment for the purposes of this Directive implies the effective exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

Whether this criterion is fulfilled should not depend on whether the network and information systems are physically located in a given place; the presence and use of such systems do not, in themselves, constitute such main establishment and are therefore not decisive criteria for determining the main establishment. The main establishment should be the place where the decisions related to the cybersecurity risk management measures are ***predominantly*** taken in the Union. This will typically correspond to the place of the companies’ central administration in the Union. If ***the place where such decisions are predominantly taken cannot be determined or*** such decisions are not taken in the Union, the main establishment should be deemed to be in the Member States ***where cybersecurity operations are carried out. If the place where cybersecurity operations are carried out cannot be determined, the main establishment should be deemed in the Member State*** where the entity has an establishment with the highest number of employees in the Union. Where the services are carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings.

64(a). ***When a publicly available recursive DNS service is provided by a provider of public electronic communications networks or publicly available electronic communications services only as a part of the internet access service, the entity should be deemed to be under the jurisdiction of all the Member States where its services are provided.***

64(b). ***In order to ensure a clear overview of DNS service providers, TLD name registries, entities providing domain name registration services, content delivery network providers, cloud computing service providers, data centre service providers, managed service providers and managed security service providers and digital providers providing services across the Union under the scope of this Directive, ENISA should create and maintain a registry of such entities, based on information received by Member States, where applicable through their national mechanisms for self-registration. The single point of contact of the Member States should forward to ENISA information. Any changes to the information should also be forwarded to ENISA. With a view to ensure accuracy and completeness of the information that should be included in this registry, Member States should submit to ENISA the information available in their national registries on these entities. ENISA and the Member States should take measures to facilitate the interoperability of such registries, while ensuring protection of confidential or classified information. ENISA should establish appropriate information classification and management protocols to ensure the security and confidentiality of disclosed information, and restrict the access, storage, and transmission of such information to intended users.***

**Article 4(1)**

(13) ‘domain name system (DNS)’ means a hierarchical distributed naming system which ***enables the identification of internet*** services and resources***, allowing end-user devices to utilise*** internet ***routing and connectivity services, to reach those services and resources***;

(14) ‘DNS service provider’ means an entity that provides***:***

***(a)*** ***publicly available recursive domain name resolution services to internet end-users; or***

***(b)*** ***authoritative domain name resolution services for third-party usage, with the exception of the root name servers;***

(15) ‘top–level domain name registry’ means an entity which has been delegated a specific TLD and is responsible for administering the TLD including the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers***, irrespective of whether any of those operations are being performed by the entity or are outsourced, while excluding the situations where top-level domain names are used by a registry only for own use***

***(15a)*** ***‘domain name registration services’ means services provided by domain name registries and registrars, privacy or proxy registration service providers, domain brokers or resellers, and any other services which are related to the registration of domain names;***

***15(b) ‘entities providing domain name registration services ’ means registrars and agents acting on behalf of registrars, such as privacy or proxy registration service providers or resellers.***

**Article 23:** ***Database*** of domain names and registration data

23(1). For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall require that TLD name registries and the entities providing domain name registration services collect and maintain accurate and complete domain name registration data in a dedicated database with due diligence in accordance with Union data protection law as regards data which are personal data.

23(2). For the purpose referred to in paragraph 1, Member States shall require that the database of domain name registration data referred to in paragraph 1 contain necessary information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs. Such information shall include:

2a. the domain name,

2b. the date of registration,

2c. the registrants' name,

2d. the registrant's contact email address,

2e. the registrant’s contact telephone number.

2f. the contact email address and telephone number of the point of contact administering the domain name in case it is different from the registrant’s.

23(3). Member States shall require that the TLD name registries and the entities providing domain name registration services have policies and procedures in place to ensure that the databases include accurate and complete information, including verification procedures. Member States shall require that such policies and procedures are made publicly available.

23(4). Member States shall require that the TLD name registries and the entities providing domain name registration services make publicly available, without undue delay after the registration of a domain name, domain name registration data which are not personal data.

23(5). Member States shall require that the TLD name registries and the entities providing domain name registration services provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall require that the TLD name registries and the entities providing domain name registration services reply without undue delay and in any event within 72 hours to all requests for access. Member States shall require that policies and procedures to disclose such data are made publicly available.

**Article 24:** Jurisdiction and territoriality

24(1). ***Entities under this Directive*** shall be deemed to be under the jurisdiction of the Member State in which they ***are established, except:***

24(a).  ***providers of public electronic communications networks or providers of electronic communications services referred to in point 8 of Annex I which shall be deemed to be under the jurisdiction of the Member State in which they provide their services;***

24(b). ***DNS service providers, TLD name registries, and entities providing domain name registration services for the TLD, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, and managed security service providers referred to in point 8 and point 8a of Annex I, as well as digital providers referred to in point 6 of Annex II which shall be deemed to be under the jurisdiction of the Member State in which they have their main establishment in the Union;***

24(c).  ***public administration entities referred to in point 9 of Annex I which shall be deemed under the jurisdiction of the Member State which established them.***