Nuremberg, 2 August 2017

Open-Xchange statement

on the public consultation on the revision of the .EU regulation

Open-Xchange would like to thank for the opportunity to express views on the future of the regulations that apply to the .EU top level domain of the DNS.

Generally speaking, Open-Xchange holds the view that .EU can and should contribute to the creation of a shared digital identity for European citizens and companies, not just in terms of e-commerce and digital market, but also in terms of **providing a unified environment for culture, information and discussion in Europe, fostering dialogue and reducing cultural and economic differences among European countries**. To this purpose, regulations should be able to assure Internet users that **a .EU service will always be subject to the laws and values of the European Union**, particularly in terms of privacy, data protection and consumer protection.

Open-Xchange would anyway like to point out a specific issue that should in our opinion be addressed in the future version of these regulations.

The technology known as **DNS Security Extensions (DNSSEC)** has been developed in the last fifteen years to counter some serious security flaws of the original DNS protocol. **Without the use of DNSSEC, any attacker – be them a criminal or a foreign power – can fool any Internet user** by providing him a manipulated DNS reply, redirecting his traffic of any kind (Web, email, etc.) to a server under the attacker's control, where **it can be easily intercepted**. In the worst case, if the "authoritative" servers for a domain name are attacked, the entire traffic for that specific domain name could be diverted to an attacker's server.

After a slow start, DNSSEC has now gained broad support as a vital security measure for the Internet. However, for DNSSEC to work, it must be supported by both the domain name registry and the domain name registrar of the domain name.

While .EU and most (not all, though) of the national European top level domain registries (ccTLDs) support DNSSEC, **its implementation and promotion by European registrars is still quite partial**. Also, while there are some European countries (Sweden, the Netherlands, the Czech Republic, Norway…) where the majority of domain names are already secured with DNSSEC, in most other countries only a minority did so; as for .EU, **the estimate is that less than 10% of the existing .EU domain names are secure**. As a comparison, while adoption is lagging behind in most of the traditional generic top level domains (gTLDs) as well, many of the newer gTLDs mandate the use of DNSSEC for all registrations, thus being effectively more secure than any European ccTLD.

This is why we think that **some regulatory action is necessary to speed up the adoption and deployment of DNSSEC** for all .EU domain names, as well as for all domain

names in European national top level domains, **to ensure that the regulatory measures taken by the European Union to protect privacy and security in online communications cannot be easily circumvented** by attacking the domain name resolution phase that precedes the establishment of any Internet connection.

More specifically, **we suggest that the regulations should establish the following principles**:

- Define a short timeframe by which all European registries and registrars will be required to support DNSSEC;
- Require registrars to turn on DNSSEC by default in all new registrations for which they also manage the authoritative domain name servers for the domain;
- Define a subsequent final deadline by which all domain names must be secured with DNSSEC.

We leave to your consideration the technical extent to which these rules should be written into a Regulation, as opposed to stating a broader principle such as *"adopting up-to-date security measures"* and deferring practical guidelines to implementation norms. Also, the .EU registry should supplement any regulation with appropriate information, suasion and training activities aimed at the operators, and perhaps even with commercial incentives as done by some ccTLDs, funding these efforts with the surplus from registrations. However, we do think that **some guiding principle in terms of DNS security needs to be stated in the Regulation**, and needs to be broadly and evenly applied not just to .EU, but to the entire European domain name industry.

We thank you for your attention and we remain available for any further question that you may have.

About Open-Xchange

Open-Xchange (OX) is a privately held company headquartered in Nuremberg, Germany, with additional local presence in Finland, France, Italy, the Netherlands, Spain and the United Kingdom, and in Australia, Japan and the United States of America.

Open-Xchange is the world's leading provider of open source messaging software and software-as-a-service solutions for hosting, service provider and telecommunications companies. OX products and services reach more than 200 million people and include Dovecot, the world's leading mail delivery agent, used by 72% of the Internet's servers to receive, store and show email to final users, and PowerDNS, the number one domain name system (DNS) software supplier in many European markets.

Open-Xchange AG is registered in the European Transparency Register at number 121349126644-88.