GDPR and domain names—restricting contact information collected via the WHOIS service (ICANN v EPAG Domainservices GmbH)

19/07/2018

TMT analysis: Senior consultant Colin Pearson, senior attorney Natascha Gerlach and associates Elisabeth Macher and Natalie Farmer, of Cleary Gottlieb Steen & Hamilton, look at a case in which the Internet Corporation for Assigned Names and Numbers (ICANN) sought injunctive relief when EPAG, an entity which registers second-level domain names decided to no longer supply certain information to ICANN on people who have registered domain names , due to concerns about the General Data Protection Regulation (GDPR).

ICANN v EPAG Domainservices GmbH Regional Court of Bonn, 29 May 2018

What are the practical implications of this case?

ICANN v EPAG Domainservices GmbH may lead to the first reference to the Court of Justice of the European Union on interpretation of the General Data Protection Regulation, Regulation (EU) 2016/679. It will be vital for data protection lawyers to closely follow the outcomes of such references, which will provide valuable guidance on the appropriate application and interpretation of the data protection principles.

The German court in this case has adopted a very strict interpretation of the principle of data minimisation (which has been an established data protection principle in Germany even prior to the implementation of the GDPR, and is similar to the principle of adequacy under the UK Data Protection Act 1998).

The court referred to the applicant's failure to demonstrate that the collection and storage of technical and administrative contact data was necessary for its purposes, due to the fact that it was possible for a registrant to use its registrant data for both the technical and administrative contract requirements. Under this narrow view of 'necessity', data controllers are precluded from optimising a process where the purpose could broadly be achieved by recourse to another (albeit potentially less relevant or accurate) data set.

What is the background to this dispute?

The applicant, the Internet Corporation for Assigned Names and Numbers (ICANN), is a non-profit organisation which co-ordinates the DNS. As such, ICANN concludes agreements with other organisations on the allocation of generic top-level domains (such as .com, .org) and second-level domains within such top-level domains (such as clearygottlieb in clearygottlieb.com). Information on persons who register a domain with such organisations is accessible to the public through the so-called 'WHOIS' service.

The defendant, EPAG Domainservices GmbH (EPAG), is an entity that registers second-level domains under an agreement with ICANN. Per the agreement, EPAG provides contact details for:

- the person registering the domain (the registrant)
- the administrative contact, and
- the technical contact for the domain

The required information for the administrative and technical contacts includes their names, addresses, email addresses and phone numbers.

Concerns arose over whether collecting this data would comply with the GDPR when it became applicable on 25 May 2018. Consequently, EPAG announced that it would no longer collect information on the technical and administrative contact, but only of the registrant itself.

ICANN filed for injunctive relief with the Regional Court of Bonn, claiming that EPAG is contractually required to provide information for all three contacts, and asking the court to order EPAG to refrain from registering domains without collecting such data.

What are the key issues involved?

The parties dispute whether collecting the technical and administrative contact information is compliant with the GDPR. Under the GDPR, personal data may only be collected 'for specified, explicit and legitimate purposes' (Article 5(1)) and must be 'limited to what is necessary in relation to the purposes for which they are processed' (principle of data minimisation, Article 5(1)).

ICANN claims that collecting the full set of data is essential to ensure the secure operation of the DNS, such as when responding to potential criminal offences or security incidents. ICANN insists that EPAG comply with the agreement, which states clearly that EPAG is under an obligation to provide those data. Additionally, ICANN argues that the WHOIS system is comparable to public trade mark registers, which have a similar purpose and likewise contain personal data.

EPAG argues that information about the technical and administrative contacts is not necessary to ensure the secure operation DNS. The current practice for registering domains allows the registrant to provide the same contact information (namely the registrant's) for all three categories. EPAG claims that registrants do so in the majority of cases. In EPAG's view, this practice demonstrates that information beyond the registrant's data is unnecessary. EPAG further argues that comparing WHOIS to trade mark registers is misguided, since trade mark registers, unlike WHOIS, are established on a sound legal basis pursuant to international agreements.

What is the current situation with the case?

The Regional Court of Bonn declined ICANN's motion for injunctive relief on 30 May 2018. It ruled that ICANN did not sufficiently demonstrate that the information required under the agreement with EPAG is essential to ICANN's objectives. The court followed EPAG's argument that collecting information beyond the registrant's cannot be essential, since it is possible to provide only the registrant's data for all three categories. Additionally, the registrant is the key person responsible for the website. While collecting additional data may be helpful in identifying or contacting the persons behind the domain, it is not necessary within the meaning of the GDPR and thus impermissible without the data subjects' consent.

Regarding the contractual obligation set forth in the agreement between ICANN and EPAG, the court held that EPAG cannot be held to this obligation insofar as it contradicts applicable law. Finally, the court also adopted EPAG's view that the setup of trade mark registers is irrelevant to the case at hand.

What is the next step?

ICANN filed an immediate appeal against the court's decision. The same court which issued the challenged decision will review the appeal. If the court decides not to grant the appeal, the case will move on to the second (and last) instance, the Higher Regional Court of Cologne.

As part of its appeal, ICANN has requested that the relevant provisions of the GDPR be interpreted by the court, with a reference being made to the Court of Justice, as necessary.

What can UK lawyers take from this case?

It will be important for UK lawyers to monitor the developments in this case and the potential future judgments of the Court of Justice—as it stands, this case promotes a very restrictive view of the principle of data minimisation which might require data controllers to re-examine the amount of data collected for purposes described and understood in broad terms. It is possible that, on further examination of the purposes for which ICANN requires technical and administrative contact data, the German court's strict interpretation will be softened.

However, to mitigate the potential risk of processing more personal data than would be considered necessary for the purpose, data protection lawyers must counsel their clients on the importance of putting in place processes to ensure that data minimisation is baked into system design, as well being a cornerstone of any organisation's data protection policies and procedures (thus complying with the obligation to ensure data protection by design and by default). Such systems and processes will need to be monitored and updated regularly to take into account any changes to the data controller's purposes for processing personal data, and/or any changes to the technological environment which may alter the necessity of data processing. Privacy notices may need to be reviewed to ensure a sufficient level of granularity with respect to the types of data processed and the individual, relevant purposes for which they are processed. Purposes described broadly, where it is not possible to identify the subtle reasons why specific data sets are needed, may fall foul of the data minimisation principle as interpreted by the German court in this case.

ICANN originally sought a GDPR moratorium from the Article 29 Working Party, in lieu of there being meaningful guidance on how ICANN could comply with the new law. The moratorium was refused and, with no guidance forthcoming, ICANN sought clarity via the courts.

In order to avoid expensive recourse to the courts in future, UK lawyers should be prepared to assist clients' efforts to lobby data protection regulators to set out practical guidance on the GDPR's application to different business practices. It may be necessary, following the publication of any guidance and/or through the decisions of national courts or the Court of Justice, for clients to change their business practices (as may be the case for ICANN). To ensure that such changes are effective, it will be vital for lawyers to work with clients to develop solutions which take into account all of the data protection principles (not only focusing on the legal basis for processing).

Interviewed by Diana Bentley.

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor.