

## European Union

### European Commission Addresses Free Movement of Health Data

The European Commission has [responded to questions raised by a member of the European Parliament](#) in relation to the free movement of data in the EU, in particular health data. The questions raised were:

- What are the main issues and concerns for the commission with regard to the free movement of data?
- How does the EU intend to remove the existing barriers to the free movement of health data across the borders of member states?
- What are the commission's priorities with regard to e-health policy and planning in the context of the soon-to-be-realised European single digital market?

The European Commission stated that obstacles to the free movement of personal data included "outdated or disproportionate regulatory requirements for keeping certain kinds of data within specific member states or regions"; "uncertainty about the legal regimes applicable to data which inhibits intra-EU flow of data"; and a "general lack of trust in the use of e-services, especially in a cross-border context". It also stated that it is working with member states to "ensure that citizens can transfer their basic medical information electronically when receiving treatment in another member state and use e-prescriptions to get their medication dispensed". Finally, it intends to adopt a communication in 2017 addressing the need and scope for further measures in the area of digital health and care, in line with the GDPR and legislation on patient rights and e-identification.

## France

### The CNIL Sanctions Two Data Breaches

In July 2017, the CNIL took action following two data breaches in relation to online platforms. Given the number of security breaches, it decided to act more severely and impose financial sanctions.

[In the first case](#), a service provider made information of more than 35,000 customers of a car rental company available online (the information included identity, address, email address and driver's license number). The CNIL considered that the company had failed to properly monitor its service provider and therefore imposed a €40,000 fine on the company. The CNIL, however, took into account the fact that the breach was corrected as soon as the company became aware of it and that it had conducted security audits.

[In the second case](#), detailed information about subscribers of a platform for car rental between individuals was accessible for three years (the information included the full name, address, telephone number, date of birth, driver's license number and location data of the vehicle offered for rental). The CNIL found that the incident was related to a basic safety fault, which the company had since rectified. The CNIL made a public warning against the company because the facts occurred before a change in law which only now authorises the CNIL to immediately fine companies without having to issue a prior notice to remedy the breach. However, the CNIL stated that it intends to impose financial sanctions for similar incidents in the future.

Both incidents have been reported to the CNIL by a website that claims to act as whistleblower system open to the public.

## UK

### Home Logic UK Ltd Fined for Making Nuisance Calls

The ICO has, once again, warned against making nuisance calls by [fining Home Logic UK Ltd £50,000 for making marketing calls](#) to individuals who had made it clear they did not want to be contacted by telephone. The company had not properly screened numbers against the Telephone Preference Service (TPS), which allows people to register their number and opt out of receiving marketing calls. Between 1 April 2015 and 31 July 2016, the ICO received 133 complaints from members of the public about nuisance calls made to their TPS-registered numbers by Home Logic UK Ltd. The ICO stated that "Organisations have no excuse – they know that calling people on the TPS register is against the law and that we will come down hard on them if they don't respect the public's right to privacy. We continue to see companies suffering the financial and reputational consequences of being caught making nuisance calls, which could have been prevented if they had invested in a TPS licence and made proper use of it. It is baffling that some firms continue to take this business risk."

## Contacts



**Philip Zender**

Partner, San Francisco  
T +1 415 393 9827  
E [philip.zender@squirepb.com](mailto:philip.zender@squirepb.com)



**Francesca Fellowes**

Senior Associate, Leeds  
T +44 113 284 7459  
E [francesca.fellowes@squirepb.com](mailto:francesca.fellowes@squirepb.com)



**Stephanie Faber**

Of Counsel, Paris  
T +33 1 5383 7400  
E [stephanie.faber@squirepb.com](mailto:stephanie.faber@squirepb.com)



**Annette Demmel**

Partner, Berlin  
T +49 30 7261 68 108  
E [annette.demmel@squirepb.com](mailto:annette.demmel@squirepb.com)



**Caroline Egan**

Consultant, Birmingham  
T +44 121 222 3386  
E [caroline.egan@squirepb.com](mailto:caroline.egan@squirepb.com)



**Emma Garner**

Associate, Leeds  
T +44 113 284 7416  
E [emma.garner@squirepb.com](mailto:emma.garner@squirepb.com)

---

The contents of this update are not intended to serve as legal advice related to individual situations or as legal opinions concerning such situations nor should they be considered a substitute for taking legal advice.

© Squire Patton Boggs.

All Rights Reserved 2017