

eHealth Hub 4th Legal workshop in London

eHealth Hub hosted the **4th instalment of its popular legal workshop** on Wednesday 22 November 2017. The presentation focused on the *Data Protection Regulations requirements for eHealth start-ups*, at the London based co-working space [Health Foundry](#).

eHealth Hub was introduced by qLegal project coordinator Clemence Tanzi (Queen Mary University of London).



The workshop was presented by qLegal and Queen Mary University of London LLM students: Wolfgang Guggenberger, Lauren Webb, Michael Chung, and Fernanda Berezovsky.

The event was well attended by eHealth start-ups who were eager to learn about eHealth Hub services, and what the future of the **new data protection regulation** entails for their businesses.

The presentation discussed the current UK legal framework under the DPA (Data Protection Act 1988), which will soon be superseded by the GDPR in May 2018, and the role of the UK domestic authority ICO (Information Commissioner's Office).

An important point of the presentation was identifying what sensitive personal data can be. The team used the example of a fictional start-ups to illustrate the overarching principles of the DPA, as well as the difference between data processor and data controller and how to navigate the new changes to the data protection landscape.



The audience was very engaged, asking precise and detailed questions throughout the presentation.

The workshop was followed by a Q&A, where the following questions were discussed:

- Is a record of vitamins consumed daily sensitive personal data?
- Who is in control of NHS data when the start-up is a third party processing the data? If the start-up is inputting their own data into the original patient record, does the right to be forgotten apply?
- Where data is anonymous even to the start-up as a data controller; is the startup complying with the right to be forgotten?
- How should an eHealth Startup deal with access requests?
- Do I need to appoint a data protection officer if my data is anonymous?
If the company is hosted in the UK, and the data is being collected from UK citizens, do the data transfer requirements apply where the data can be accessed in a non EU country for reasons of customer support or developer need to access it? Is it "accessed" if it is only seen not transferred? What consent do I require when I sell data to a third party and am I liable for access requests where this third party defaults on their obligations?

If you would like to receive updates on eHealth Hub developments and future events, please register at <http://www.ehealth-hub.eu>.