Europe *EU*

Data protection and "smart" products: a new perspective on safety

More and more "smart" consumer products are being made available on the market by a hugely diverse range of companies. These smart products already offer remarkable functionality. And as they become increasingly sophisticated, they will contain features that would have seemed like science fiction just a few years ago. While this technology space holds out enormous opportunity – both commercially, and for improving many aspects of people's lives – it comes with risks, especially where reliance on a data-driven model is concerned.

Already well versed in processing customer data, many companies will have put in place systems to cope with the regulatory demands for personal data protection. Others may be well established in the technology space, but less familiar with the dynamic of getting products into consumers' hands. And then there will be companies that are completely new to the market – disruptive start-ups, moving at high speed to launch their innovative products ahead of the competition.

It's vital to put safety and cyber security front and centre during any smart product launch – especially for products that rely on the use and processing of personal data. This article focuses on one of the key reasons why: the General Data Protection Regulation (the "GDPR"), which governs personal data protection in the EU and has a major impact on how companies introduce smart products to the market.

What Do You Need To Know About The GDPR?

In force since May 2018, the GDPR's overarching aim is to simplify and harmonise the data protection and privacy regulation landscape across Europe. It created a single set of rules that

- enhance the protection of EU data subjects, including giving data subjects greater control over the use, storage and retention of their personal data
- put greater focus on practical compliance through "data protection by design" and by ensuring companies document compliance
- have extraterritorial reach – just because a company does not operate in the EU, or do business in EU countries, does not mean the GDPR won't apply, and
- grant strong enforcement powers to the European Commission (fines of up to €20 million, or 4% of global turnover, whichever is the highest).

The GDPR applies to all companies that collect or use personal data. That includes information collected at the point of sale, information collected from a consumer to optimise a product's performance, and all personal data in between. Product companies are likely to hold huge amounts of data that will be subject to the GDPR's rules. Typical sources include

- consumer contact details obtained during the course of sales, signing up to mailing lists and marketing materials
- usage data relating to products
- cookie data (user's geolocation or IP address) obtained from website visits, and
- data enabling or optimising a product's performance.

Consumers are increasingly aware of the value placed on their personal data. And, on the back of numerous high-profile corporate data breaches, they understand companies' obligations when it comes to protecting their data. This is felt particularly acutely where smart consumer products are concerned: customers expect their data to be handled safely and securely while also expecting the operability of the product that relies on the very processing of that personal data to be of the highest standard.

At first glance, it may be difficult to see the value in investing in data protection, especially when there are so many other competing challenges facing businesses in the current climate. However, the ubiquity of data in today's world and the potentially catastrophic impacts of getting it wrong, both in terms of regulatory fines and brand damage, should alert decision-makers to the importance of data protection across all consumer products companies.

Successful companies in this space embed data protection principles in everything they do, ensuring that it features as prominently as other more "traditional" risks (such as physical product safety).

How Can Companies Get It Right?

Through their drive to become GDPR-ready, most smart product companies will already be very familiar with data protection and privacy. Listed below are some of the headline topics they have likely addressed.

Gathering personal data

In any scenario where personal data is collected, compliant collection mechanisms must be in place. The scenarios triggering this requirement may not always be obvious and can include, for example, where a customer has made an enquiry or where they have provided consent for data to be collected and used to optimise a product's performance.

All sources from which a customer's personal data is being collected by the business should be identified and companies should ensure collection mechanisms are compliant.

Legal bases

Companies must state the legal basis for gathering personal data and keep a record of the stated basis. There are six permitted bases, all included in article 7 of the GDPR; however, in the context of consumer products, the two most likely bases are consent and "legitimate interests".

Wherever possible, the "legitimate interests" basis for data collection should be used; this avoids the problem of a later withdrawal of consent. In the context of product safety issues, the "legitimate interests" basis should be built into the stated purposes under which all personal data is collected.

Data protection by "design and default"

Data protection "by design and default" is required by the GDPR. This means that companies must have appropriate systems and procedures in place to ensure that data is neither collected excessively nor misused. Where data processing is likely to result in a high risk to individuals, a formal data protection impact assessment ("DPIA") must be carried out to identify any mitigating measures that need to be taken.

Retention practices should be reviewed against the data minimisation rules; data should only be kept for as long as necessary to achieve the stated purpose for which it was collected. The retention period will vary according to the product and could, for example, be informed by usage data that might show a period of inactivity, leading to a trigger for data deletion.

Data subject rights

The key rights of a data subject are

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing
- the right to data portability
- the right to object, and
- rights relating to automated decision-making and profiling.

Companies should be mindful of an individual's right to access and request the deletion of their personal data. Most requests will have a 30-day maximum period for response, and companies must put in place the resources and systems needed be able to handle such requests promptly. Companies and their employees should be particularly aware from the outset that an individual may one day see all the information collected about them, so high standards of communication diligence should be encouraged throughout the business.

Cookies

The GDPR has changed the position of the ePrivacy Directive in that "opt-out" consent is no longer a sufficient justification for the use of non-essential cookies. To justify non-essential cookie use, the GDPR requires that consent must be clear, affirmative, and involve the consumer "opting in". Non-essential cookies include those used for marketing, advertising and analytics. It must also be as easy to withdraw consent as it is to give it.

In practice, companies often make access to their website conditional on the user's acceptance of non-essential cookies. It remains to be seen whether this approach is permissible in the eyes of the regulator,

or whether they will take a strict stance in interpreting the GDPR's consent requirements. A reasonable assumption would be that consumer rights and safety regulators will resist the imposition of conditions which restrict either the consumer's ability to exercise their rights, or to access safety information posted on a website. This means that where safety information or usage instructions can be found on company websites, and where customers can lodge warranty claims on the website, the customer should have full access, without any requirement to accept non-essential cookies.

GDPR in times of a safety event

The corrective actions taken in the wake of a safety incident must also comply with the GDPR. The ideal scenario is for a company's data collection practices to allow for customers to be contacted directly if a safety event occurs. Where this is not the case, or where the customer data is not being held, companies must ensure data collection and processing is GDPR compliant, applying the necessary technical and security controls to the use and retention of that data.

Companies must also ensure that any third parties engaged to assist with corrective actions, such as logistics companies or third-party communications agencies, handle personal data in a safe and secure way, limited to the execution of the corrective action. To ensure a swift and effective incident response can be executed, these checks should ideally occur proactively before the occurrence of a safety incident.

Data breach and reporting

Companies must have robust protocols for detecting, investigating and reporting on data breaches. Where such a breach is accompanied by a safety risk – for example a car's on-board computer system could be hacked, resulting in brake disablement – the company will have to consider the relevant reporting requirements of both the data regulator and the relevant safety regulator. The triggers for reporting and the processes for doing so will vary across regulators. If the incident is multi-jurisdictional, the company will have to satisfy the requirements of multiple regulators (each with different protocols and reporting deadlines), while also carefully handling media and reputational issues. Given the propensity of regulators to talk to each other, the consistency of messaging is crucial, as well as the need to ensure a clear and coherent company response.

Companies should be aware that a failure to report a breach can, by itself, result in a significant fine. On top of regulatory liability, the company could face civil claims for the misuse of personal data if security systems are deemed inadequate.

Comment

The GDPR was introduced with the protection of consumers firmly in mind, so it follows that consumer product companies will be under the spotlight from regulators.

On the whole, when it comes to data security and privacy, companies should place as much emphasis on these issues as they would on more 'traditional' product safety liabilities. In such a complex field, with products subject to myriad intersecting regulatory requirements, product companies that keep an eye open to regulatory and commercial developments are most likely to thrive.

Valerie Kenyon
Partner, London
T +44 20 7296 5521
valerie.kenyon@hoganlovells.com

Anthea Davies
Senior Associate, London
T +44 20 7296 5251
anthea.davies@hoganlovells.com

With thanks to Ranulf Barman