

# Cybersecurity and data protection by design

*Implementing compliance in product development*

## Legal obligations

The legal requirements for the implementation of cyber security in products (cyber security by design) are complex, diverse and dependent on the type of product in question. However, in view of the increasing threat of cyber attacks, corresponding requirements exist for almost every product. The General Data Protection Regulation (GDPR) also plays an important role in the processing of personal data.

## What are the penalties for violations?

Monitoring the legal requirements for cyber security and data protection in products is the task of the market surveillance and data protection supervisory authorities. Violations may result in sales bans, recalls, destruction orders and public product warnings, as well as fines and orders for the deletion of personal data. In addition to regulatory consequences, there may also be the threat of civil damage compensation claims.

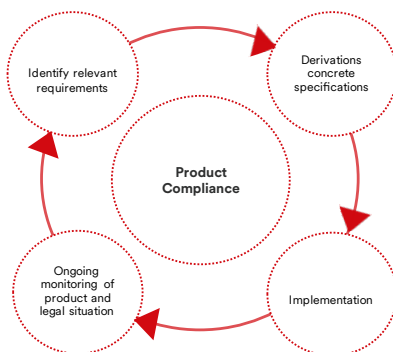


Figure 1: Product Compliance © reuschlaw, 2023

## Product compliance

In our experience, it becomes possible to implement legal requirements in product development when this takes place within

a product related compliance management system.

The following aspects should be considered in particular:

- clear identification of legal requirements
- proper selection of technical and organisational measures
- and the relevant technologies
- documentation of the implementation and compliance with requirements
- continuous monitoring for changes in the legal situation

## Next step: Contact us

Take the first step on the road to product compliance now and arrange a one-on-one meeting with us.

We will present our concept for implementing cyber security and data protection in product development to you in detail, answer your questions, and create a suitable offer for your company.

T + 49 681 / 859 160 0

E [info@reuschlaw.de](mailto:info@reuschlaw.de)