

---

---

# 7 Lessons in Data Regulation Learned from GDPR

*by i2Coalition and eco*

Good intentions aside, the GDPR came on the scene as a complex, 150-plus page document that many found lacked helpful, practical commentary on how to apply the regulations to their particular circumstance. While many businesses who went through the process are blocking out the memory of GDPR-related meetings and reworking various business processes, we found some examples of how these data regulations could have been better implemented while still achieving the same underlying goals.

## 1. No Exemptions for Small Businesses and Associations

The GDPR does not provide for exemptions for small businesses and associations, which would be appropriate, as they have neither the staff nor the know-how to internalize all requirements and implement them promptly and properly.

Large companies can spin up entire GDPR departments which would be disproportionately more costly for small companies, meaning this one-size-fits-all approach gives huge companies a competitive advantage over smaller ones.

If the GDPR had been rolled out differently, regulations could have only applied to companies exceeding a specific revenue or another measure of size.

## 2. No Group Privilege

Companies that belong to a group are not seen as a single storage entity under the GDPR. They are treated as separate units. The exchange of data within the group is therefore not permitted without further ado. For example, sending personal or customer data via e-mail to a foreign base of the same group is a data transmission where data protection applies. For data transfers to third countries, EU standard contractual clauses and/or binding corporate rules apply.



The i2Coalition is the voice for businesses that build the Internet. This includes cloud providers, data centers, domain registrars, registries, and other foundational Internet enterprises.

[i2Coalition.com](http://i2Coalition.com)

[contact@i2Coalition.com](mailto:contact@i2Coalition.com)  
(202) 524-3183



With more than 1,100 members, eco is the largest Association of the Internet Industry in Europe.

[international.eco.de](http://international.eco.de)

[info@eco.de](mailto:info@eco.de)  
0221-70 00 48-0

---

### 3. More Education Work Needed

The supervisory authorities have largely abandoned German companies in the implementation of the provisions of the GDPR. Assistance and process templates were published too late or not at all. If these had been present in advance, many misunderstandings could have been prevented (for example, blackening of photos in kindergartens, on whether names can still be printed on bell labels).

### 4. No Distinction between B2B and B2C

The GDPR does not provide a distinction between B2B and B2C, but treats everyone equally. Work between companies therefore involves significant bureaucratic effort. For example, If somebody follows the GDPR very accurately, they would have to inform the transferor of a business card already at its receipt about all relevant rights and processing activities etc.

### 5. The GDPR Promotes a Risk-Based Approach

The more risk there is for the data subject when there is a data breach, i.e. the more sensitive the data is, the more is required to protect the data technically and organizationally. However, the GDPR does not offer guidance on how to implement this. This means that companies run the risk of being sanctioned if the measures they take are ultimately not considered sufficient given the risk, and this in turn leads to the risk of being more restrictive than required.

### 6. Inconsistency Caused by National Legislation

The intention behind the GDPR was to harmonize the legal landscape in Europe, but there are a lot of clauses where national legislation may apply. This fragmentation by country is contrary to what the GDPR was designed to do.

### 7. Guidance on How Non-EU Controller/Processor Sanctions can be Imposed

The GDPR has a global reach when the data of EU data subjects is processed. In order to be effective, explanatory language in the GDPR or the recitals would have helped clarify how sanctions could be imposed on non-EU controllers or processors.

## Lessons for Future Data Laws

As other jurisdictions revise their existing data laws and create new ones, we can look to the rollout of the GDPR to guide the creation of effective regulations that do not unduly burden organizations, yet also achieve their intended consequences of solidifying trust.