Open Access Government April 2019

Co-location data centres and privacy regulations

What do you need to consider as a customer when it comes to co-location data centres and privacy regulations? Green Mountain Data Centres Ltd tell us more

As a data centre, we are used to answering a number of questions from our potential and existing customers. The questions traditionally concern power, cooling, sustainability, connectivity, and physical security measures, but lately more and more people ask us about privacy regulations as well. The introduction of the General Data Protection Regulation (GDPR) in European Union (EU) in 2018, and it's potential €20 million[1] penalties for breach, have made companies very focused on being GDPR compliant. So how does GDPR affect your company if you trust a co-location data centre to store your data?

Where does the GDPR apply?

Let's start with the basics – what is GDPR and where does it apply? In simple terms, GDPR gives people more control over their data and businesses benefit from a level playing field. The GDPR not only applies to organisations located within the EU but also to organisations located outside of the EU if they offer goods or services to or monitor the behaviour of EU data subjects.

But what about Norway, which is not a part of the EU? Having our data centres in Norway makes no difference. Norway is a member of the European Economic Area (EEA) which means we are also subject to the GDPR regulation and have also incorporated it in our own national privacy regulations. To conclude, if you store personal data on servers in data centres in Norway or other EEA member countries or the EU, you are subject to GDPR. Norway not being part of the EU should not be a factor to consider when choosing a data centre location in Europe.

Who is responsible for compliance?

In order to explain this, we have to look closer at two important terms in the regulation – the data controller and the data processor. The data controller determines the purpose of the processing of personal data, in what way it should be done and that data is processed in accordance with the requirements of the GDPR. A data processor processes personal information on behalf of the data controller. The data processor has independent responsibility for having satisfactory information security to protect the personal data. The data processor may only process personal data in accordance with what has been agreed with the data controller.

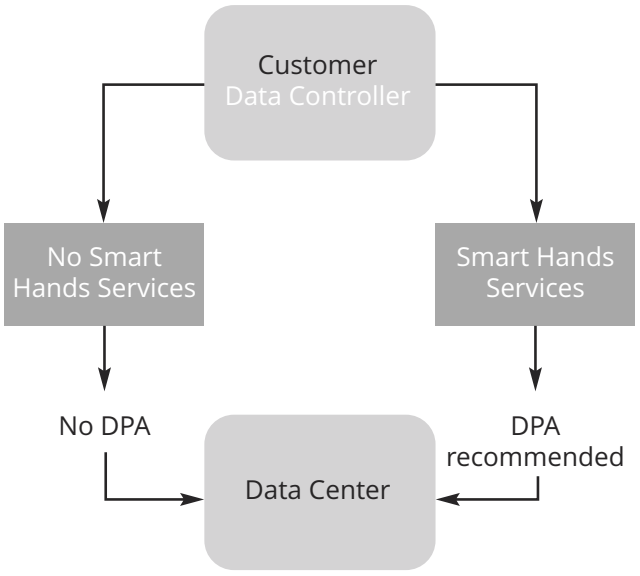
Clients at a co-location data centre can be controllers or processors or both. Some clients are data controllers who have placed their personal data about clients, employees etc. in our centres. Others are data processors, for instance, service providers or cloud companies, who process the data on behalf of multiple customers inside the data centre. The relationship between the data controller and the processor is governed by a Data Processing Agreement (DPA). The data controller is responsible for compliance and must make sure they enter into data processing agreements when necessary.

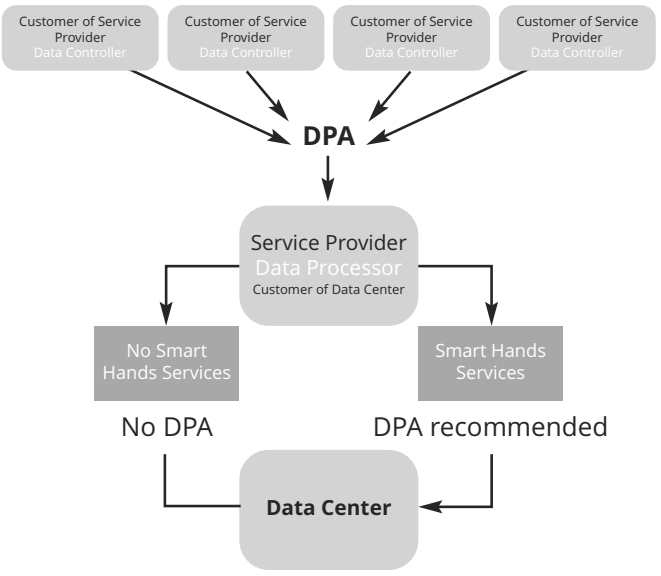
Do you need to sign a DPA with your data centre?

In general, the answer is "no", but there are exceptions. It all depends on what kind of services your data centre performs. The basic offering of a co-location data centre is the IT infrastructure – the space, power, cooling, security, and connectivity. None of which affects the processing of the personal data stored on the customer's servers. Let us look at two different scenarios:

Scenario 1: The client has its own servers and equipment, even its own personnel, and the co-location delivers the infrastructure mentioned earlier. The data centre employees do not even have access to the data rooms unless authorised by the client. In such cases, a DPA is not required, but an ordinary contract between the client and the data centre should cover the requirements relating to securing the infrastructure.

Scenario 2: On the other hand, some data centres, like Green Mountain, offers "Smart Hands" services to their clients. These services may include technical personnel getting access to the server and the possibility to log on. In theory, they would have the possibility to access and process personal data. In that context, a DPA between the parties could be considered.





A GDPR compliant data centre?

The responsibility of handling personal data in compliance with GDPR is in the hands of the data controller. They have to make the right decisions regarding the choice of service/cloud provider or data centre. Knowing that the data centre itself operates in accordance with GDPR would be a trustworthy sign when choosing a data centre partner. As an example, Green Mountain is a data controller of various personal data; we handle personal information regarding our employees, our clients, visitors, and our client's personnel who access the data centre. We use CCTV to monitor the facilities and conduct a strict ID control in order to access the data halls. Green Mountain also needs to be committed to ensuring that these subject's privacy is protected. All our procedures are designed to comply with regulations, and we have conducted a thorough Data Protection Impact Assessment (DPIA) to support it.

What about the Cloud Act? What about Brexit?

Many of Green Mountain's clients are international, and we experience that concerns relating to the U.S. Cloud Act and Brexit are recurring topics. The Cloud Act means that US authorities may require U.S. cloud service providers to disclose data, which may appear to be in direct conflict with parts of GDPR. This issue is currently being debated by the European Data Protection Board. However, this will have a greater impact on data centres owned by the cloud providers themselves. If they use a co-location facility owned by another company, it may be harder to enforce the Cloud Act in the EU and EEA.

The other topic is Brexit; do companies need to be compliant when it is unknown what will happen to GDPR in the UK after Brexit? If a company processes data about individuals in the context of selling goods or services to citizens in other EU countries, then it will need to comply with the GDPR, irrespective as to whether or not the UK retains the GDPR post-Brexit. If activities are limited to the UK, then the position is much less clear. The UK Government has indicated it will implement an equivalent or alternative legal mechanism. The expectation is that any such legislation will largely follow the GDPR, given the support previously provided to the GDPR by the ICO and UK Government as an effective privacy standard, together with the fact that the GDPR provides a clear baseline against which UK business can seek continued access to the EU digital market.

In a data-driven world, the concern for privacy is becoming increasingly important. All organisations handle personal data in some way or another and should place great emphasis on complying with regulations. Having clients that question and challenge us on these topics is a sign that companies take this seriously, in every aspect of their business.

References

1 Up to €20 million, or 4% of the worldwide annual revenue of the prior financial year, whichever is higher.

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

https://www.datatilsynet.no/en/

http://www.lexology.com/library/detail.aspx?g=07a6d19f-19ae-4648-9f69-44ea289726a0

https://www.congress.gov/bill/115th-congress/house-bill/4943/text

https://eugdpr.org/the-regulation/gdpr-faqs/

Green Mountain

Green Mountain Data Centres Ltd
Tel: +47 51 50 96 10
https://greenmountain.no/