Preventing the datastrophe: why your data's protection policy matters in negotiations

Written by Florina Pop, Lukas Adomavičius, Frank Lavadoux and Olivia Brown

Preventing the datastrophe: why your data's protection policy matters in negotiations

A few months ago, we discussed what cybersecurity measures should be put in place to prevent intrusions during video conferences, and before that, we explained the concept of cyber diplomacy. This time we invite you to delve into the issues of data protection. You might wonder how cybersecurity and data protection are different, and why data protection matters in negotiations. To give you a short answer, cybersecurity covers safety against cyberattacks. In contrast, data protection covers personal data protection, proper personal data processing safeguards, data management, access prevention, conformity with data protection laws and much more. These two concepts are different yet very much interlinked.

Data protection is the very basis for a successful online negation process: it is essential to ensure that the video conferencing platform you are using processes your data in conformity with the GDPR, that your online agenda does not process your data in a harmful way or your clients' documents are stored safely – the list is endless. To visualise that, think about your driving licence. It is irresponsible to drive without it because this action will carry consequences for you and at the same time, it will affect others' safety. It all leads to one point – working and negotiating online without proper data protection standards is dangerous and costly. That is why for this blog, we decided to introduce you to the most crucial aspects of data protection to keep in mind.

Why does personal data protection matter?

Personal data is ever more important in a society that is nowadays driven by data. Even the simplest tasks online rely on your personal data being processed: be it for ensuring security, or for companies to monetise your personal data to earn profit by suggesting personalised ads. Personal data can reveal a lot about an individual. So naturally, it can also be exploited to harm you. The now infamous statement that the Covid-19 pandemic has changed the world and how we work, also applies to the personal data protection field.

Companies and individuals now rely on cloud systems to store their data; video conferencing and online collaboration tools are crucial for daily work and negotiations with partner companies. That is why being aware of data protection standards is essential to ensure that your data is processed safely and legally. Also, data protection breaches highly influence the image of your company and its competitive advantage, and implies extra costs. Nobody wants to use services or conduct business with an organisation deemed to be not in compliance with data protection standards. So the question remains, how do we ensure proper data protection techniques and avoid the picture of being unreliable?

The holy grail – General Data Protection Regulation

The answers related to your data protection questions can be found in the General Data Protection Regulation (GDPR). Of course, many of you heard about it, most probably when agreeing to the cookie policy or consenting to receive marketing emails, but what does GDPR actually require, and what specific actions can you take to ensure you and your interlocutor's data safety?

Most likely, your organisation employs a dedicated person responsible for data protection measures – Data Protection Officer (DPO). GDPR requires the appointment of a DPO for every public authority, an organisation that process large amounts of data or process special categories of data. The DPO should be your contact point if you have any questions about data processing, be it simple and obvious or complex – we should not rely only on our own understanding of how to navigate the digital world. However, there are steps to be taken by you to ensure safe data processing, an easier life for a DPO and protection of your organisation's data.

Data protection in times of working from home

Besides the fact that we are returning to our usual work practices, the Covid-19 pandemic changed our typical work organisation. More and more of us combine working remotely together with regular office days. Organisations have developed new ways to access data, which increases the risks of data breaches and makes it harder to identify it. Consequently, it is crucial to develop policies to mitigate the increased risks and keep your organisation and everyone in it safe.

The first step to consider is developing personal data protection procedures for remote work. It should address minimum security requirements that take into account the needs and objectives set by your organisation. Suppose your organisation allows for a *Bring Your Own Device* policy or only a *Company-Owned, Business-Only Device* policy. In that case, these different methods should be clearly addressed in the personal data protection procedures, and relevant safeguards should be imposed. Of course, that is something to be addressed by your organisation. However, the data is safe when these procedures are addressed both from an organisational but also technical point of view. For example, for remote work directing network traffic through the firewall/intrusion detection, even in the case of home office or mobile work (e.g. by using VPN connections to organisational security mechanisms when accessing the internet) is paramount. That is why raising concerns to the management level of your organisation in case of the absence of any procedures is highly recommended.

Treat other's data as your own

First, keep a record of your data processing activities. You might be wondering, why? As in our analogue world, we need to know where your data is, who and how is working with your data and how that can impact your work. This is even more important due to the increased number of third-party service providers that we use because of Covid-19. We conduct our online negotiations through different online channels, meaning that in one way or another they all collect your data.

Data mapping is a crucial component of GDPR and is considered to be a foundation step to fulfil legal requirements set by the GDPR. Before data processing, your customers have to be informed in a transparent way about the fact that their data is being processed, meaning that your company has to specify how is this going to be done, for which purposes and for how long. That is done to allow your organisation to organise, catalogue, manage and structure data, and maintain adequate records of data processing activities. In addition, it is crucial for organisations to map all contractual instruments of the company which envisage international transfer of data, outside the EU or EEA. This is needed to identify and assess the risk and additional safeguard measures your organisation may need to put in place to legally transfer the data. For instance, if you wish to start using a new online tool, imagine online conferencing or a new online space for storing collaborating with your colleagues, you should first request this/inform your DPO or an IT department before using it. This is so that, when necessary, a proper data protection impact

assessment is conducted before you download and use the new online tool.

Every detail, even the smallest, counts

Second, ensure proper data security safeguards. Most likely, you will have to rely on your IT department to do most of the job, but on the other hand, your IT department depends on you acting responsibly online and as per the data protection and data security training. Be careful with emails or websites you open; be aware of various types of cyberattacks or other ways hackers can exploit you. Another important aspect to keep in mind is to notify your IT department or a DPO of a possible data breach. This step is crucial because your organisation can be unaware that its data is not safe in some instances. If you notice any irregular activity, do not wait. Additionally, data breaches include the safety of hardware. For instance, a lost USB stick has to be reported to your organisation – every detail, even the most minor, counts.

One last thing, what about surveillance by the employer?

We should not forget the other side of the coin of implementing data protection procedures in your organisation. One of the considerations is that your employer might take advantage of increased data protection awareness – intentionally or unintentionally – and track how employees use company devices. There are numerous software tools to track devices; for example, it can identify how much time are you spending in front of the computer or log every movement you make with your computer mouse. Keep in mind that this kind of personal data processing is problematic through the lens of GDPR, and it might be hard if not impossible for your employer to justify it.

Are you interested in expanding your knowledge in the field of data protection? Subscribe to keep updated on our activities.

Read blog one, two, three (part 1), and (part 2), four, five, six and seven, eight and nine of the series 'Possible impacts of the current pandemic on international negotiation processes' by the Negotiation Team.

Do you have questions? Contact the Negotiation Team negotiationteam@eipa.eu.

The views expressed in this blog are those of the authors and not necessarily those of EIPA.