When Your Personal Data Becomes Everyone's Property

Sille Larsen Nielsen

How the EU adopted a legal framework to protect their citizens' personal data from being misused or carelessly handled, and to what extent Bhutan can benefit from these (hard earned) experiences.

In May, 2018, the European Union implemented a common set of data protection laws — General Data Protection Regulation (GDPR) — revolving around the individual's right to privacy and freedom, laws which have drastically changed the way in which personal data travels and the discourse around it. Non-EU businesses are losing European partnership contracts because they cannot guarantee adequate protection of data complying with GDPR, the governments and businesses in EU member states have been forced to take on a larger responsibility in safeguarding the data, and ordinary young people, who thought they were "just" sharing a Facebook video with strangers in it, are being prosecuted and fined.

This article aims to briefly dip a toe into the sea that is GDPR. Through case examples, I wish to share some of the reasons why GDPR was necessary, explore what it could (possibly) mean for Bhutan, and what recommendations I can offer, both to the country in ensuring technological and organisational security and also to its citizens in their everyday use of personal data. Being a Danish citizen and primarily working with data protection in Denmark, my examples will be mostly drawn from these experiences.

What is GDPR?

We cannot start a dialogue on GDPR without briefly explaining what it is and why it was necessary to launch it. "Personal data" is defined as any information relating to you as an individual and which can identify you directly or indirectly. It can be your name, address, your location data, photos of you or more sensitive data concerning your health, religion, ethnicity, fingerprint, eye scan, even your biological samples and DNA. It is your data and you should have a say and control over what it is being

used for. A common misconception is that GDPR prevents governments and companies from collecting, using, and sharing personal data. That is not what GDPR does. It says: "You can do all these things but you have to follow a set of rules and take on a responsibility."

The travel of information knows no national borders. Denmark and the rest of the EU member states have learned that you need common legislation to frame how citizens' personal data are used, who is allowed to collect it, share it, and publish it. And at the centre of all this stands my rights as an individual; to be informed when someone is using my personal data and in a way that I can actually understand, to have access to my data if I ask, to have inaccurate data rectified and to have my data deleted if I withdraw my consent. These are just some of the fundamental rights GDPR provides EU citizens.

I have a friend who casually declared that she did not care what websites tracked her Internet habits or whether her insurance company had gained access to her health record (without her consent that is). Her somewhat spoilt reaction was built on the premise that she lives a peaceful life and what could anyone possibly want with her personal data? Well, if you are thinking the same, let me burst your bubble right now. Your personal data is very valuable, not just to target advertisements but to predict how you will vote, how likely you are to become a parent, your travel and consumer patterns or your life expectancy.

I do not have to go very far to find examples of governments collecting data on their citizens in order to be able to identify (and arrest) people of opposite political views, or where voting regulations were profiled, with the intent of excluding certain groups from voting altogether, or where companies are so careless with protecting your personal data that hackers easily gain access to it. It can lead to a lack of confidence in your state representatives, to a public display of damaging photos on Facebook, or even placing someone's life at risk.

Ten years ago, you would be considered a conspiracy theorist if you expressed wonder at how the advertisement on a website so uncannily resembled a private online chat conversation that you had the previous day. Not anymore. GDPR aims to give you, the individual, the largest possible control of your personal data while overcoming an overwhelming lack of transparency.

Even if you — before GDPR — wanted to know what your personal data was used for, you as an individual had little or no feasible means to translate the "terms and conditions" of, for example, websites before accepting. And I do mean translate, because the terms are written in such long and incomprehensible texts that you do not even realise that you had just given some app the right to your personal chat history, or data from additional apps on your phone.

Any EU business owner or government body that collects, stores or shares personal data on individuals needs to comply with GDPR, guarantee the rights of the individual, and implement appropriate technical and organisational security. If they decide to outsource work to third party companies (which is perfectly fine and many do) they are responsible for ensuring that the third parties have adequate protection in place before sharing the personal data. As you can imagine, this is not easy and has caused a lot of bureaucratic headaches and communication issues.

Before we embark on my recommendations for Bhutan, one last thing on GDPR must be said. Although the regulations aim to protect individuals, individuals themselves do not have to comply with them. The collection of personal data for your own private use (pictures you take, notes you write, etc.) is not affected by this. GDPR is aimed at government bodies and companies, not you as a person. That would be far too restrictive. It is only when publishing personal data on others, or using it for business purposes (including posting photos on social media) that we need to worry about GDPR.

Will It Affect Business and Government?

It does not have to. There are several scenarios in which your business or government organisation in Bhutan is not all affected by GDPR. It can be that you simply do not have any business with European companies or public bodies, or that your business with them does not require that you have access to personal data of EU citizens.

If, however, you do need access, you need to figure out what that means for you. It depends on the specific job you do and how sensitive the data is, etc.. The best way to understand the consequences for you is to ask your European partner. It is their job as the Data Controller (the one who

collects the data and decide what to use it for) to assess if their business with you makes you a Data Processor in the eyes of GDPR (performs a task on the Data Controller's behalf).

Let me give you an example. Local governments in Denmark are responsible for providing home care for elderly people. For this task, the local government needs an appropriate IT-system to keep track of all the personal data they collect on the elderly receiving home care, the kind of medication they receive, the specific help they need, their contact details, etc.. The local government does not have the skill set required to create and code such an IT-system, so they buy an exciting system, which the fictional company CareForYou has developed. CareForYou is based in USA, and even though all the data is stored on servers in Denmark, CareForYou still has access to the system, since they need to implement security updates and such. It means they also have access to personal data on elderly people in Denmark. Since CareForYou wants to do business with a Danish local government, they have to provide guarantees that the company has appropriate technical and organisational security to safeguard the data. Otherwise, what is to prevent them (besides good intentions) from selling that information to third parties?

If you, through dialogue with your European business partner, decide that you are in fact a Data Processor under the terms of GDPR, you have to be able provide sufficient guarantees. I can only recommend looking at the European Commission's "standard contractual clauses": it is a set of terms and conditions which may serve as an inspiration to you.

Beware, though, that there are a few strict requirements that Bhutanese national legislation needs to accommodate, and which will affect you, if your business with EU member states involves processing personal data on EU subjects (be it storing, transferring or even just accessing). You need to be able to guarantee appropriate security, also from your own government.

One of the challenges that GDPR and US companies face concerns the US Patriot Act. This specific US anti-terror legislation provides the US government, under specific circumstances, the right to access personal data on EU citizens stored on US servers, without informing the subjects (e.g me). And although the US government keeps promising that it is not the intent of the Patriot Act to accommodate spying, some EU countries and companies are withdrawing their US-based cloud services altogether.

Sharing Photos and Compromising the Privacy of Others on Social Media

The first time I visited Bhutan was in 2008 during the first ever democratic elections. Due to my age (23 at the time), I made friends with many local youths through evening parties, movie nights, and hangouts, etc.. In my experience, there was a real concern and healthy awareness that the wave of globalisation and technological expanse can also bring with it, if allowed to roam uncontrolled, a vulnerability and loss of control over what is private and what is not.

Danes could indeed learn something from the healthy scepticism the Bhutanese youths were demonstrating. In 2018, Denmark held the podium as the most digitalised country in the world.[1] Digitalisation is so ingrained in the Danes' everyday life that it dominates how we go about our existence and communicate.

On my phone right now there is an app with live updates of all my banking transactions, and through which I pay for everything. I literally have not held cash for years, but instead, I whip out my phone and hold it against the cash register. Even if I shop, I have five different apps for that as well. I have had an app for my official digital post-box since the authorities and private companies, by law, stopped sending physical letters altogether.

Let us not forget my app for declaring my taxes, for sending pictures to my doctor (so I do not have to show up in person), for checking homework assignments, for tracking my friends' GPS locations, for buying bus and train tickets, for dating, for signing documents (instead of with a pen), and for punching in my work hours. All of this information is connected. So, when I register that I have worked for eight hours today, or I am taking a sick day, a digital robot automatically sends that information to my employer. There, it is received by yet another digital robot who shares it with its robot friends at the tax office and the bank. It makes it really hard for me to cheat on my taxes.

And we have not even discussed social media yet. Every company, and all of my friends, post photos and videos all the time, often without considering whether they need consent from the subjects. In the EU, if you publish photos of someone where they might be considered to be in a damaging or

[1] https://publicadministration.un.org/en/Research/UN-e-Government-Surveys

protected situation, you actually need consent. This can be people at work or at a private function drinking a beer.

You almost always need consent to publish photos of children or vulnerable groups such as homeless, refugees, or handicapped. And not just Facebook, Instagram, Snapchat and YouTube, because there are so many apps available. I work in IT, and every time I look at my 13-year-old niece's phone, she has five new social media apps or games downloaded that I have never heard of. They all offer instant gratification through likes, scores, and annoying sounds.

All that personal data being collected on me is overwhelming. GDPR is about protecting my personal data, including photos and videos. There has been — and somewhat still is, because these things take time — a blind culture of sharing photos and videos of oneself, friends, and family. Or of someone we do not even know. We watch compilations of funny videos on YouTube and share them before questioning if the people in them are minors, or if the footage can be damaging to them. It is nearly impossible to stop the sharing of photos, and maybe that is why so many do it without considering that it might not only be damaging for the subjects, but also illegal to share.

In 2018, the Danish police charged over 1,000 young people, most between 15 and 18 years, for distributing a specific intimate video over Facebook and Messenger. It has been dubbed "the Umbrella case". In the footage, a girl aged 15 was having intimate and private relations with the opposite sex. Without her knowledge, the footage was shared online. Instantly, the video became infamous and shared like wildfire among schools and students.

The experience, besides being extremely humiliating and degrading, almost ruined the girl's life. Deciding to set an example — that it is, in fact, illegal and extremely damaging to the subjects of such videos — the Danish police gained access to Facebook's log files and obtained a list of all who had forwarded the video to someone else. As one investigative officer said: "We are under the impression that young people are well aware of the consequences for victims of sharing material of this kind. But they possibly do not know that it is illegal."

So why did it happen? Some say that the girl should not have done the act.

Others proclaim that anyone who takes embarrassing or private photos of themselves should know better. But it is not that black and white. We will never be able to control what people do in the privacy of their homes or prevent someone from making a fool of themselves at parties. But making mistakes does not justify public shaming or forfeiting the right for control of their personal data.

I am so grateful that no one had Facebook back when I went to high school and no one took pictures of every embarrassing moment throughout my most vulnerable years. I am thankful that I get to shape the image of myself that I want my employer, my parents, children, and partner to have.

In Denmark, and so many other places, there is a culture of sharing: phones in hands all the time, taking pictures, sending to your friends. Laws set in place to prevent this are always 10 years too late and adults' opinions of avoiding it — or "just don't take embarrassing pictures" — is absolutely antiquated. You need proper dialogue, not just restrictions and pre-judging.

Denmark is one of the most digitalised country in the world, and we have only now just put Digital Behaviour on the school curriculum. Do not make our mistake. Bhutan has smart, strong-minded and entrepreneurial youths, and they deserve a dialogue. All us oldies (I am 34 and I feel ancient in this discussion) could learn something by listening to them and understanding why digital communication and visual sharing is such a big part of their lives.

Laws Alone Will Not Get the Job Done

GDPR is quite a mouthful: It contains 99 articles and, compared with Bhutan's Information Communication and Media Act (ICMA) from 2018[2] — which, among other issues, also targets data protection — GDPR can seem like a supertanker. However, I would claim that the ICMA only provides Bhutan with a minimal data privacy protection and lacks many of the important aspects from GDPR.

For someone whose main occupation is implementing GDPR, I find the EU laws a little breathtaking, but I understand why they are necessary. There is a whole chapter on what my rights are, and several chapters on the

[2] https://www.dit.gov.bt/information-communications-and-media-act-bhutan-2018

responsibilities of the Data Controller and what they need to do in case of a data breach. We have had many data breaches — sending letters to the wrong recipient, accidentally publishing a memo containing confidential names, or using a service provider outside of the EU without proper contracts.

GDPR is, however, not ruthless. It does allow for some space for manoeuvres. If you are a small company which only collects names, addresses, and a few other personal data on maybe a few hundred people, you do not need the same strict security measures as large local governments, which collect very sensitive data in vast amounts. It also allows for some photos taken in public by the media to be published without consent.

GDPR contains a set of guiding principles for all data processing which can be hard to apply sometimes. One principle says that the collection of personal data is only allowed to take place in accordance with a specific and lawful task, but when that task is in the exercise of official authority, the Data Controller does not need the consent of the subjects. They still need to tell me about it though. But what does that mean in real life and what are the limitations?

You need supplementary guidelines helping you to translate the law into practical examples. If you want ordinary business owners and non-paralegal staff to actually follow a data protection law (be it GDPR or Bhutan's ICMA), you have to offer guidance, and not years after the law has been implemented.

My overall recommendation is, data protection is foremost a communications project. It is about changing our way of thinking about our own and other people's personal data, as well as educating our private and government organisations to take on the necessary responsibility. You cannot expect them to do that without guidance, and without talking to the very people who are processing personal data — both the business owner and her teenage children.