"*Historically, privacy was almost implicit, because it was hard to find and gather information. But in the digital world, whether it's digital cameras or satellites or just what you click on, we need to have more explicit rules – not just for governments but for private companies*". Bill Gates

Privacy is not an option, but rather a necessity, and should never be the price we pay to access the internet.
Almost every aspect of our lives revolves around data, and almost every service we use involves the collection and analysis of our personal data.

Therefore, in this ever-evolving digital era where data can be easily accessible or hacked, what is the importance of private data, how can individuals protect and keep their data private, and what are the consequences should they not?

Data privacy has always been valuable. That is why people rent safe boxes in banks, and lock their filing cabinets. However, the more data becomes digitized, and the more information is shared on the web, the more important data privacy becomes.

Personal data is very important. It helps companies develop business models, conduct effective marketing campaigns, understand their customers and develop various products and services accordingly. Yet, companies should protect this data and use it in a very responsible way, in order to prevent third parties from misusing it in fraud, or identity theft.

In fact, we have witnessed several cases of personal data breaches worldwide such as Facebook, eBay, Adobe, Yahoo, and Equifax, whereby personal data (such as social security numbers, addresses, credit scores, etc,…) of millions of individuals was violated.

A regulation called The General Data Protection Regulation (GDPR) was introduced in Europe in April 2016 (and became enforceable in May 2018) in order to set the standards of how businesses and organizations should handle the private information of individuals they interact with. It affirms that an individual's personal data belongs to the individual, and imposes

substantial fines on companies not abiding by the rules. These fines can go up to EUR 20 million or 4% of a company's worldwide turnover, whichever is higher.

The main objective of the GDPR is to give control back to EU citizens and residents over their personal data and protect their privacy, as well as to simplify the regulatory environment for international business by unifying the regulation within the EU.

In order for companies to comply with the GDPR rules, here are some examples of what to do:

- Inform individuals about the company's activities in a transparent manner, and clarify to them why the company is processing their personal data. For this reason, companies should post Privacy Notices and Privacy Policies on their websites, and modify their agreements to include GDPR clauses.
- Manage, through a Data Processing Agreement, the controller / processor relationship, which is a relationship with all third party organizations, agents, contractors, or other parties working on behalf of the company.
- Assign a Data Protection Officer (DPO) for the company whose responsibility is to oversee the company's data protection strategy and its implementation to ensure compliance with the GDPR.
- Keep a record on the use of data
- Manage efficiently the rights of the individuals, and be ready to act quickly in case any individual wants to exercise his/her right according to GDPR. Those rights are as follows:

  The right of an individual to access his / her personal data, to receive a record of the data that the company holds, to have the data corrected in case of errors, to have the data deleted if certain criteria are met, to have the data transferred under certain circumstances, and to object or restrict certain uses of the personal data.

- Set up procedures to handle personal data breach within 72-hours, and identify the steps a company needs to take in order to minimize risks, and notify the concerned individuals as well as the supervisory authorities.

- Review and assess the impact that every new activity / product may have on data subjects, and analyze the possible risks through a process called a Data Protection Impact Assessment (DPIA).

In fact, every individual should be concerned about data privacy and not consider that data privacy is just a business concern. The more individuals know about data privacy, the better they will be able to protect themselves from a large number of risks.

Individuals should not think that there is a trade-off between security and Privacy. In fact, Technology allows having both.

Here are some simple tips to help individuals protect their personal data:

1. Use a locking mailbox at home, so that fraudsters cannot steal the mail.
2. Shred discarded documents, including receipts, as well as bank and credit card statements that contain personal information.
3. Secure the home Wi-Fi network and other devices so that cyber criminals cannot spy on an individual's online activity.
4. Use strong, unique passwords for all of online accounts.
5. Use a Virtual Private Network (VPN). VPNs provide online privacy and anonymity by creating a secured, private network from any Internet connection, whether accessed from a home Wi-Fi or from a public Wi-Fi hotspot.
6. Regularly assess the privacy settings on social media accounts.

In conclusion, Data will become even much more valuable in the next coming years than it is today. Therefore, the more efficient we store and protect our data, the more it is beneficial for our businesses, companies, and ourselves.

By: Nadine Ghosn

Founder and CEO – BeyondComply