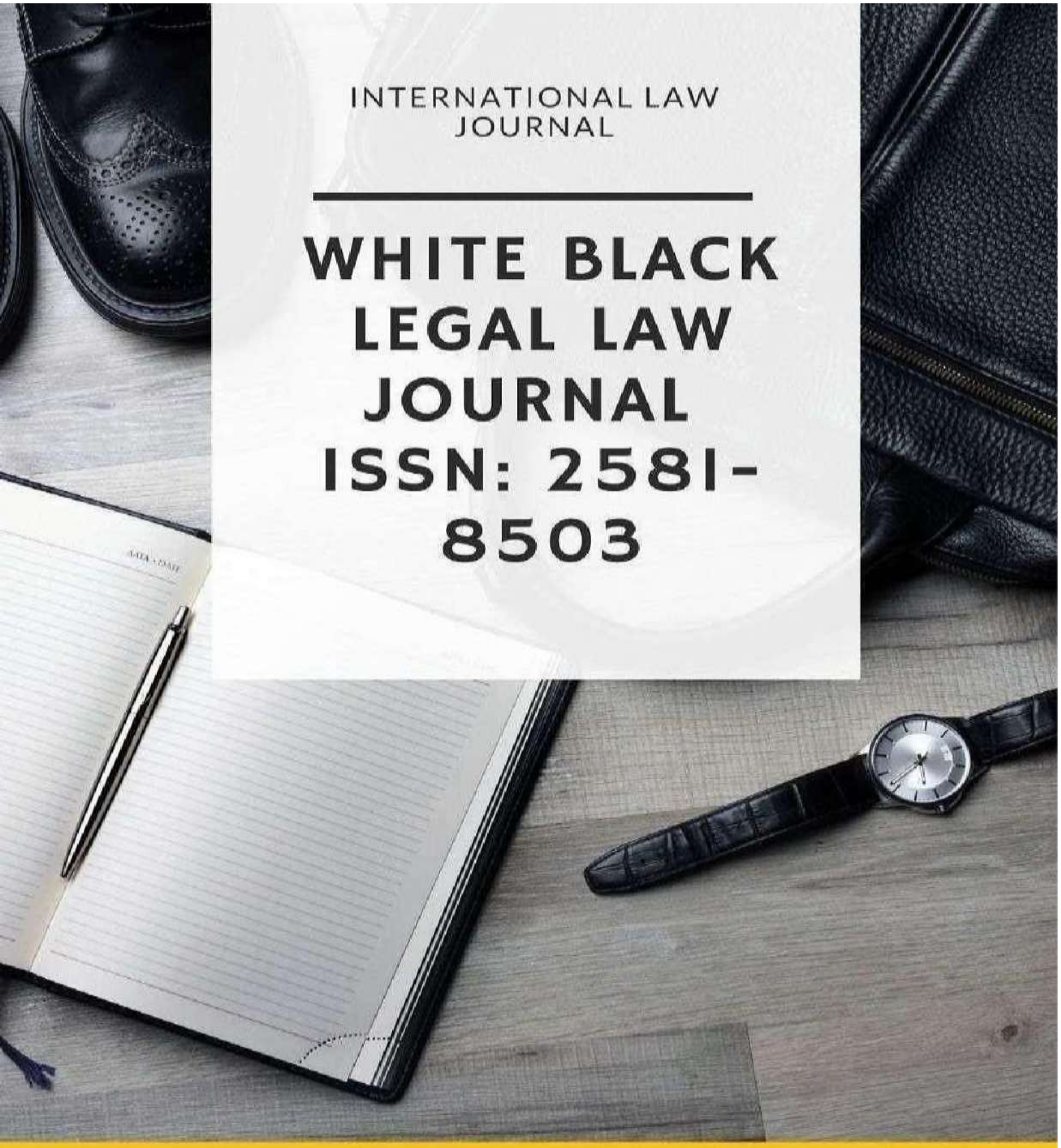

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

www.whiteblacklegal.co.in
Volume 3 Issue 1 | May 2025 ISSN: 2581-8503

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

GDPR- A GAME CHANGER IN DATA PROTECTION LAWS FOR THE DIGITALIZED WORLD

AUTHORED BY - DIVYA.R

ABSTRACT:

The year 2012 heralded the beginning of 4 years of concentrated legislative efforts in the field of personal data protection in the EU that culminated into the EU voting for the implementation of the GDPR[1], and finally lead to the publication of the GDPR in the Official Journal of the EU, in April 2016[2].

The concept of personal data protection, however, was not a novel one. October 1995 witnessed the adoption of the EC Data Protection Directive (EC/95/46)[3] (the ―DPD‖). For years, the DPD continued to be the gold standard, as it were, in personal data protection lexicon.

So, what brought on the need for a new legislation, there were several factors that came into play. The DPD was felt to be archaic as technology had advanced in leaps and bounds since 1995. In the words of Elizabeth Denham, the UK Information Commissioner, Regardless of the rate of regulatory change, data- related technology advances more rapidly. Moreover, despite the fact that the EU Member States had transposed the DPD and the barriers to the free movement of personal data between the Member States had been removed, there were still too many legislative differences between the Member States, which led to disparities in how the DPD was implemented throughout the EU. Due to lack of adequately funded or resourced enforcement efforts, compliance to the DPD was ―patchy‖ at best, causing multiple and increasing numbers of data breaches.‖ Data controllers took advantages of the above, and, therefore, business practices became more aggressive with personal data being

[1]―Microsoft, _Overview of the General Data Protection Regulation (GDPR)‘ [2017] Information Commissioner‘s Office <https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/>.‖

[2]Fair Digital Economy and others, _Introduction‘(2018) 4 European Data Protection Law Review 0 <https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/>.

[3]Rebecca Wong, _The Data Protection Directive 95/46/EC: Idealisms and Realisms‘ (2012) International Review of Law, Computers and Technology657.

misused/abused. Additionally, if one were to be honest, it seemed that the data subjects had very little actual control over the use of their personal data.

Overall, it was established that DPD in its current form would not last long. The weaknesses identified were, as follows[4]:

- Unclear linkage between "personal data" and actual privacy risks;
- The measures implemented to provide greater transparency were inconsistent and ineffective;
- The rules on international data export and transfer were archaic to say; the least;
- International data transfer was a cumbersome task;
- "Patchy" and "inconsistent" role of the Data Protection Authorities (DPAs);
- Other minor glitches that led to faulty implementation.

To address the aforementioned, it was felt that instead of completely overruling the DPD, it would be in everyone's best interests that the current arrangements be leveraged upon in a better manner, and that the current rules be implemented better. Pursuant to this, the first GDPR draft proposal was released in January 2012. In the following years, the draft was revised multiple times leading up to the final draft (in its present form) being eventually published in 2016.

Whilst Chinese astrologists might have been calling the year 2018 as the Year of the Dog, for a lot of people, 2018 proved to be the Year of the GDPR. May 25. 2018 — let's call it a watershed event in the history of data protection — witnessed the enforcement of the GDPR. In the months preceding and following May 25, 2018, we have seen the ripples of the stone inflicted by the GDPR globally, with EU Member States and other countries following suit in

[4]Douwe Korff, _EC Study on Implementation of Data Protection Directive 95/46/EC‘(2011) SSRN Electronic Journal 65.

transposing the GDPR into local legislation. Let us start with how the GDPR has apparently transformed the way we look at personal data protection.

3.1 GDPR versus DPD — a Sea-Change?

To the seasoned privacy practitioner, the changes do not seem too big. However, it would do us a whole lot of good to be wary of the GDPR, as there are significant changes and several new requirements[5].

If it has to be summed up the changes brought on by GDPR whilst comparing it to the EU DPD:

- Increased territorial scope;
- More stringent consent obligations;
- New data subject rights;
- Increased accountability;
- Revisions to international data transfer;
- New legal liabilities;
- Significantly greater penalties.

All of the above translates into more onerous obligations on the part of data controllers and data processors, and a far more punitive enforcement regime when it comes to non-compliance with the GDPR.

This is captured below in an easy-to-read table:

Basis	**Data Protection Directive (DPD)[6]**	**General Data Protection Regulation[7] (GDPR)**

[5]Actiance, _GDPR Compliance and Its Impact on Security and Data Protection Programs‘ (2017) IEEE Wireless Communications. 709
[6]Neil Robinson and others, _Review of the European Data Protection Directive‘ (2009) Rand Europe Technical Report.
[7]Bocong Yuan and Jiannan Li, _The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation‘ (2019) International Journal of Environmental Research and Public Health 551.

Wider Territorial Scope (or, the net is cast wide)	DPD applied to instances where personal data was processed within the EU or by using equipment located in the EU	GDPR, in addition to EU based companies, also applies to companies offering goods and services to EU citizens.
Holistic & Comprehensive (or, the cliched one-step shop)	Under the DPD, companies were answerable to the DPAs of the respective EU countries of establishment	In instances where the company has an EU office, the GDPR mandates a single supervisory authority (a lead DPA) in order to address data protection complaints across all EU Member States.
Consent (or, please make it a resounding YES)	In the era, personal data of subjects was obtained via implicit actions, opt-out boxes, and pre-ticked boxes.	Under the GDPR, the permission bar was raised and made much more stringent. Consent must be freely granted, particular, informed, unequivocal, and provided by explicit and affirmative action.
Penalties, (or, taking a punishment)	―Black points‖ under the DPD included both civil and criminal sanctions, forfeitures,	The GDPR imposes severe penalties, including fines of up to €20 million or 4% of a

	and fines up to EUR 250,000.	company's global annual revenue in the preceding financial year, whichever is greater.
Privacy by Design and by Default (privacy cannot be just a footnote)	Under the DPD, data protection and security mechanisms were unregulated, with privacy being a mere reference point.	Under the GDPR, companies will be required to embed privacy and data protection as a default action point into the initial designing of data processing activities.
Data Protection Officer (DPO) (or do you need a beat cop?)	Under the DPD, there was no mandate on whether a beat cop (read, DPO) should be appointed.	Mandate for Organizations/ companies carrying out processing of large-scale data of special categories to appoint and keep a DPO.
Data Controllers vs Data Processors (or as you sow, so shall you reap)	The DPD provided for a punitive regime for data controllers with data processors being out of bounds in most instances. Furthermore, if procedures were being followed, even data controllers were not considered liable for downstream (read,	The DPD stance now stands significantly transformed with the GDPR laying massive legal (and, more onerous) obligations at the door of the data processors. In fact, even data controllers will now be held liable for the non-compliance of

	service providers or data processors) processing errors.	data processors, in which they will have to pay the fines, whilst suing the data processor for damages caused)
Breach Notification Mandate (or, —give a bell‖)	The DPD did not set forth express legal obligations to report data breaches. It did, however, indicate that serious data breaches be notified.	The GDPR mandates that in-scope companies report —high risk‖ breaches to regulatory authorities and data subjects within 72 hours of the breach coming to their knowledge.
Data subject Rights (—Here enhanced rights to my data now‖)	The DPD set forth limited data subject rights, as follows: (1) limited right to erasure of PD – suppressed results of internet searches only. (2) right to access to personal data was ambivalent – no clear obligations on data controllers with regard to period and format of data to be given to the data subject; (3) no mention of data portability.	The GDPR makes data subjects rights broader and legally enforceable, as follows: (1) Rights of access. (2) Right to rectification (3) Right to erasures (4) Right to restrict processing (5) Right to object to processing. (6) Right to data portability.

3.2 The GDPR: An Analysis

The GDPR, without an iota of doubt, is an ambitious piece of legislation wherein the magnitude of predictable transformation is substantial. However, it does not have to be all Hydra-like, or the monster that it is largely perceived to be. Set forth here are some of the salient points that one must bear in mind while implementing privacy programs that are aligned to the GDPR[8].

1. Extraterritorial reach/nature of the GDPR

Although the GDPR fundamentally governs businesses set up in the EU; it also covers companies set up outside of the EU, offering goods and services to, or monitoring data subjects/individuals in the EU. Companies outside of the EU have to appoint a representative which has to be present in the EU (subject to limited exemptions), wherein the representative shall bear responsibility/liability for any breaches[9].

2. Core mandates around data protection are the same

The GDPR continues to be the same as the DPD in that the core mandate around processing of personal data are the same. It covers the acts of both data controllers and data processors. The 6 general principles of data protection make an appearance here as well, and companies must satisfy processing conditions/bases; however, there are significant new changes to the principles and the data processing conditions that one must be wary of. The definition of sensitive personal data is now expanded to include genetic and Homeric data.

3. Consent

Consent continues to be one of the justifications for processing of personal data; however, valid consent is now harder to obtain. Moreover, data subjects can now withdraw consent at any point

[8]European Commission, _Principles of the GDPR‘ (*https://ec.europa.eu/*, 2018) Accessed on 27 March 2020. [9]Sangwoo Lee, _A Study on the Extraterritorial Application of the General Data Protection Regulation with a Focus on Computing‘ (2019) SSRN Electronic Journal 233.

of time. Both in the case of sensitive personal data and for data transfers outside of the EU, explicit consent is required. With regard to provision of online services to a child, consent from a child will only be valid when authorized by a parent. The GDPR defines a child as a 16-year-old. This age can be reduced up to 13 years by Member States[10]. Additionally, there are more security provisions afforded to children, for example, the situations where the "legitimate interests" condition of processing may be used have been limited – this is to say that a child's "right to be forgotten" is now stronger and more fortified.

4. Data subjects' rights

This is an area that has been brought to the forefront more than ever before with the implementation of the GDPR. While the existing rights relating to rectification of inaccurate data, objection to direct marketing, challenging automated decisions, etc., remain, there are several new and enhanced rights, like, the right to erasure (or, the right to be forgotten), the right to portability of data, etc[11]. These new rights are like knotted strands now, and a company will need to have proper response mechanisms in place to address these.

5. Privacy notices

Privacy notices are now required to have multiple information points, as required by the GDPR, much more than before. One would think this would be case, but here's the quandary – bigger isn't necessarily better! Your notices will also have to simultaneously be concise and be able to make sense to the laymen[12]. It should skip the legalization and the jargon!

6. Accountability

Being compliant or saying that you are complying is fine, but can you demonstrate compliance? Being able to demonstrate compliance means conducting privacy impact assessments where required (in cases of high-risk processing, especially), having adequate technical security measures in place, etc. In order to show that you are, indeed, compliant, you may even have to sign up to a code of practice or be certified.

[10]Milda Macenaite and Eleni Kosta, _Consent for Processing Children‘s Personal Data in the EU: Following in US Footsteps?‘ (2017) Information and Communications Technology Law 108.
[11]PT Wolters, _The Control by and Rights of the Data Subject under the GDPR‘ (2018) Journal of Internet Law 97.
[12]Mike Hintze, _Privacy Statements Under the GDPR‘ (2019) Seattle University Law Review 796.

7. Data Protection Officers

Based on the kind of data processing that companies carry out, and the magnitude of their operations, they may be required to appoint a ―data protection officer‖ (DPO). These DPOs are your subject matter experts in all aspects of data privacy and should be consulted for all data protection matters in the company[13]. DPOs are to report directly to the "highest level of management" within the company and cannot be penalized or terminated for doing their jobs.

8. Data security

GDPR suggests enhanced mechanisms like encryption, etc. Additionally, companies must pay heed to the data breach reporting requirements[14] (unless a breach is unlikely to cause a risk for individuals, companies must report data breaches to their supervisory authority ―within 72 hours‖).

9. Obligations of data processors

Right when data processors were sitting safely ensconced in their BPOs, call-centers, KPOs, LPOs, other IT structures, the GDPR decided to expand the list of obligations that these processors will have to bear the burden of, directly, and in their contracts with data controllers when it comes to claims by data subjects/individuals. Data processors can now be held jointly and severally liable along with data controllers[15]. Companies outside of the EU, who set themselves up as data processors earlier to escape such liability, can no longer plead innocence or ignorance.

10. International (outside the EU) data transfers

[13]Martin Brodin, _A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises‘ (2019) European Journal for Security Research 343.
[14]Tony Ke and K Sudhir, _Privacy Rights and Data Security: GDPR and Personal Data Driven Markets‘ (2020) SSRN Electronic Journal 114.
[15]Information Commissioner‘s Office, _Overview of the General Data Protection Regulation (GDPR)‘ (2017) Information Commissioner‘s Office 412.

For data transfer outside of the EU, companies will have to ensure that certain conditions are met. Rules with regard to such international transfers[16] continue to remain tough to comply with.

— There are some minor exemptions, but they aren't of much use, practically.

3.3 Decoding the GDPR Rubric

In the countdown to May 25, 2018, and thereafter, the GDPR[17] continues to leave us and scratching our scalp. It might seem like a contagion to our collective imagination. How is one to survive the contagion communication of disease from one person or organism to another by close contact and its aftermath?

First step is to stop thinking of it as an epidemic, and instead, turn this into an opportunity to ensure that the data of individuals that is kept, and processed is secured at all times. This will change the way individuals and your holders look at you and will increase your brand value in the market. It's quite simple. Get your head out of the cloud of articles, blogs, commentaries about how difficult and cumbersome the GDPR is, and just think about the simple ways in which you can assure your employees, suppliers, clients, etc., that data is safe with you. Thinking about your stakeholders and not just the penalties imposed by the GDPR will make things a lot easier. As the data privacy experts at Linklaters put across quite succinctly: Privacy counsel will need a bit more consideration, a great lot of pragmatism, and a dash of bravery.

3.4 National Derogations

One of the main drivers for the GDPR to come to the fore was the need to have an able and harmonious data protection framework across the EU. Hence, the GDPR is directly effective in all of the EU without the Member States having to

[16]Hiep Tran, _Briefing on Data Processing and International Data Transfer in Accordance With GDPR‘ (2020) SSRN Electronic Journal 54.
[17]Sahar Bhaimia, _The General Data Protection Regulation: The Next Generation of EU Data Protection‘ (2018) Legal Information Management 63.

implement national laws. However, there are, and will remain, several divergences, as there are so many elements of the GDPR that are bound by national legislation; we also have to bear in mind that different countries have varying cultural and social approaches towards data protection. Additionally, there are differences in the ways the different supervisory authorities will implement and enforce the GDPR in the respective Member States.

1. DPOs - it is up to Member States to make DPO appointment mandatory.
2. Children – Member States can reduce the age of consent (online services) for a child from 16 to 13 years old.
3. Employment – More stringent restrictions can be imposed by member states on processing of employee data.
4. National security – Member States can limit rights afforded to data subject/individuals in areas that concern national security, judicial proceedings, and crime.
5. Freedom of information - Member States can amend the GDPR so that the idea of data protection is reconciled with that of freedom of information. For example, Member States can restrict processing of national identity numbers, and protect information that is subject to professional secrecy.

Further, national law governs many processing activities. For instance, one of the bases for the processing of personal data happens to be to meet an obligation under Member State law; or that processing of information about ―criminal offences‖ is only permitted when allowed by Member State law; or that the ―right to be forgotten‖ does not apply if such processing is required by Member State law; or that a Member State recognized public interest can be used to transfer data outside of the EU and; that Member States can impose additional and more stringent restriction on international data transfers[18].

Due to the foregoing technological advancement, one cannot hope to have the impact of the GDPR fully harmonized all over the EU.

[18]Tran (n 16).

3.5 Extra-territorial Nature/Reach of the GDPR

If a company is set up or established in the EU, the GDPR will apply. It could be a branch or even a subsidiary; just that there should be effective and real activity via the use of stable arrangements in the EU. However, the GDPR shakes things up and extends the reach of the data protection law to companies based outside of the EU. If you are a company in India and offer goods and services to people in the EU, you are caught in the GDPR net[19]. Additionally, if you monitor the behavior(s) of individuals based in the EU, the GDPR applies to you. It just refers to individuals being tracked online for profiling purposes. So, if you are a business, based in India, but you profile customers are based in the EU and are offered personalized recommendations based on such profiling, then you could be a business falling within the purview of the GDPR. The GDPR applies to you if you track individuals across multiple sites or use applications, etc., to track geo-locations[20].

Now, you may naturally have concerns regarding what supplying products and services to EU residents entails. Does this mean that if you have a website that can be accessed by people based in the EU, you fall within the ambit of the GDPR? Not really. Several variables come into play when considering whether your actions constitute the provision of goods and services to EU residents. Following is some of the instances which become subject to the GDPR based on "offering goods and services" to individuals in the EU[21]:

1. Using the language that is not even relevant in your own country—for example, if you are an Indian website, but you are using German.

2. If you show prices in Euros whilst Euros is not even used in your home country.

[19]Shakila Bu-Pasha, _Cross-Border Issues under EU Data Protection Law with Regards to Personal Data Protection‘ (2017) Information and Communications Technology Law 83.
[20]ibid.
[21]Benjamin Greze, _The Extra-Territorial Enforcement of the GDPR: A Genuine Issue and the Quest for Alternatives‘ (2019) International Data Privacy Law.

3. If the top-level domain name that you are using is that of an EU Member State (e.g., de for Germany).

4. If you are delivering physical goods to an address in, say, Hungary.

5. If your website includes references to Norway-based customers using your products.

6. If a huge percentage of your customers is based in the EU.

7. If you pay for advertisements to be published in a Member State newspaper, whilst your base of operations is the US.

However, just accepting a credit card payment that has an EU billing address does not mean you have to comply with the GDPR. Electronic delivery of goods and services to an individual based in the EU does not automatically mean that company will have to comply with the GDPR. If the internet advertising is seen by individuals in the EU but is not targeted at them[22], the GDPR does not apply. Just because the telephone numbers provided in the website have international prefixes, the GDPR does not automatically apply to you.

The website may also have to comply with the GDPR if they are dealing with a data controller or processor based in the EU; and also, if they are providing services to a data controller or processor who in turn offers goods and services to individuals in the EU.

To the extent that the extra-territorial provisions of the GDPR apply the website will need to appoint a Representative (it could be a group company) based in EU, in the Member State in which the relevant data subjects are based. One does not have to appoint a representative, however, if the data processing is once-in-a- while in nature, or if such data processing is unlikely to cause risk to individuals, or if there is no large-scale processing of sensitive personal data.

[22]Douwe Korff, The Territorial (and Extra-Territorial) Application of the GDPR With Particular Attention to Groups of Companies Including Non-EU Companies and to Companies and Groups of Companies That Offer Software-as- a-Service' (2019) SSRN Electronic Journal 113.

3.6 Lawful Processing

Processing of personal data on lawful grounds is not a new requirement, of course, but it's important to refresh the concept. For Lawful personal data processing, it should comply with all general data protection principles[23], and it must be backed by at least one of the six grounds for processing. If there is sensitive data processing, then at least one sensitive data processing condition must be met.

3.7 GDPR's 6

Here's a quick reckoner on the 6 general data protection principles that were a part of the DPD, as well.

1. Lawfulness, fairness and transparency- Companies must ensure that they process personal data in a manner that is lawful, fair, and transparent[24].

2. Purpose limitation- Companies must collect personal data for purposes that are specified, explicit, and legitimate[25], and should not be processed. Further than the identified purposes (unless it is for public interest, or for historical, scientific, and research purposes).

3. Data minimization—Companies must collect/process only as much personal data as is required to fulfill the purpose behind the processing, in that the personal data is ―adequate, relevant, and limited‖ to the identified purpose[26].

4. Accuracy[27]—Companies must ensure that the personal data that they collect is accurate, and that it is kept up to date. Companies must either rectify or delete inaccurate personal data.

[23]Elena Gil González and Paul de Hert, _Understanding the Legal Provisions That Allow Processing and Profiling of Personal Data—an Analysis of GDPR Provisions and Principles‘ (2019) ERA Forum 321.
[24]ibid.
[25]Himanshu Arora, _Grounds for Lawful Processing of Personal Data in GDPR and Personal Data Protection Bill 2018, India (PDPB): Section – VII: Employment Purposes‘ (2021) SSRN Electronic Journal 245.
[26]Gil González and de Hert (n 23).
[27]ibid.

5. Retention—Companies must ensure that they keep personal data in an identifiable format only until the time that the identified purpose is served, or in accordance with statutory record retention obligations[28] (exceptions relate to public interest, historical, scientific, or statistical purposes).

6. Integrity and Confidentiality[29]—Companies must ensure that personal data is kept safe and secure, and does not fall prey to unauthorized disclosures, breaches, attacks, etc.

3.8 Grounds for the Processing of Personal Data

Ensuring that grounds for processing of personal data are lawful is not a new requirement. However, with the GDPR coming into effect, it becomes imminent to understand and be able to record these grounds and ensure that they are within the realms of legality. To be considered as processing personal data lawfully, one should have at least one of the following baser grounds covered.

1. Consent—Consent has to be obtained by the ―data subject for one or more specific purposes‖ while processing their personal data.

2. Necessary for the performance of a contract-It is necessary to process data to perform a contract, or where data subject is a party to a contractual obligation, or at data subject's request certain steps need to be taken before entering contract.

3. Legal obligation—The processing is deemed necessary to comply with a legal/statutory requirement that applies to the data controller.

4. Vital interests—Processing is considered essential to defend the vital interests of the data subject or of another natural person.

5. Public functions—Considered required for the performance of a job in the public interest or the exercise of official power vested in the data controller, processing is deemed necessary.

[28]Arora (n 25).
[29]Gil González and de Hert (n 23).

6. Legitimate interests—For the purposes of any legitimate interests of the data controller or a third party, processing is deemed necessary except where any such interests are countermanded by the interests of the data subject or the fundamental rights and freedoms accorded to the data subject which require the protection of personal data, especially in instances where the data subject is a child.

There is this popular fallacy that one must obtain individual consent in order to process data lawfully. Truth is that it is not a pre-condition to lawful processing; it is also not a way to circumvent processing activities that would be considered lawful in general. That being said, however, will need consent for other processing activities—for instance, if you intend to send unsought emails or texts a recipient, you will mandatorily require their specific and explicit consent.

In order to bank upon "legitimate interests", you must ensure that you have legitimate business reasons to process personal data. And, you have to ensure that such legitimate interests are not countermanded by the data subject's interests and their rights/freedoms. Furthermore, if you are going to use the legitimate interest‘s base, you must mandatorily disclose this to the data subject, via a privacy notice (also referred to as fair processing information).

To the extent that you want to further process personal data already obtained for another purpose that was not set forth earlier, you must verify that your new purpose is not completely a mismatch with your older/original purpose of processing. This means that you should compare the purposes, review consequences arising out of the processing (actual and intended), and review safety mechanisms (existing and future) in order to secure the personal data.

Notwithstanding the above, where it comes to processing of special categories of data (personal data relating to race, religion, sex life, health, and political, and genetic and biometric information), you are prohibited from processing such data except in fairly limited circumstances—such circumstances would include where you have obtained the "explicit" consent of the data subject, the

processing, is deemed necessary legally, of where the processing is for reasons of public health and interest.

Processing of data relating to criminal convictions and offences based on a one of the lawful grounds mentioned above must be conducted under auspices of an official authority, or as authorized by EU or a Member State; that provides for adequate and appropriate safeguards.

As per the GDPR, public authorities will no longer be able to use the "legitimate interests" condition and will have to bank upon one of the other conditions (most likely, the public functions condition). This could potentially include not just state entities, but also private entities that provide public service, for example utility companies.

3.9 Grounds for the Processing of Sensitive Personal Data

When it comes to the processing of sensitive personal data, the GDPR has far more stringent restrictions. Although there are more than 6 conditions, these are extremely narrow and far more difficult to base data processing upon. In order to process sensitive personal data, companies must be able to meet at least one of the following 10 conditions[30]:

1. Explicit consent—Sensitive personal data can be processed by organizations if the data subject/individual has given ―explicit consent‖[31]. However, EU or Member State law may limit the instances in cases where such consent is already available.

2. ―Legal obligation related to employment‖—Where processing of sensitive personal data is obligatory to fulfill legal/statutory obligations arising out of employment law[32], or is required under collective agreement.

[30]ICO (n 14).
[31]Māris Bomiņš, _Consent As A Legal Basis For Processing Of Personal Data‘ (2019) Administrative And Criminal Justice 88.
[32]Arora (n 25).

3. Vital interests—Processing of sensitive personal data is to be done to protect vital interests of the data subject or those of another natural person, for example, in case of medical emergency.

4. Not-for-profit bodies—Processing of sensitive personal data is done by non- profit body way of legitimate activity; data remains with the members of that body or other related persons; data is not disclosed outside of that body without data subject's consent.

5. Public information—The processing of those sensitive personal data which data subject themselves has made public.

6. Legal claims—Processing of personal data is required to prove or defend legal claims, or when courts are acting in a judicial capacity.

7. Substantial public interest—When substantial public interest is involved processing of sensitive personal data is required based on EU or Member State law(s).

8. Healthcare—Processing of Sensitive personal data is deemed necessary for healthcare purposes but must be suitably guarded[33].

9. Public health—Processing of Sensitive personal data is deemed necessary for public health purposes based on EU or Member State law(s).

10. Archive—Processing of sensitive personal data is deemed necessary for archival, scientific, or historical investigation, or statistical[34], and such processing is based on EU or Member State law(s).

3.9.1 Yes, I do / accept – Consent

[33]Mary Kirwan and others, _What GDPR and the Health Research Regulations (HRRs) Mean for Ireland: ―Explicit Consent‖—a Legal Analysis‘ (2021) Irish Journal of Medical Science 107.
[34]Olly Jackson, _GDPR Readiness in the Spotlight‘ (2017) International Financial Law Review 113.

Even though consent is a cornerstone of the GDPR, one cannot rely solely on consent as a ground for processing of personal data. In fact, it would be difficult, foolhardy, and inefficacious to do so.

That being said, though, consent does serve a slew of purposes under the GDPR, it is one of the lawful grounds for processing, even for processing special categories of data[35]. It can also rely on as an exception from the restriction on data export/transfer outside the EEA. One will need it for some of direct marketing activities. However, such consent must be explicit. It cannot be obtained through a course of conduct or be implied.

Note, however, that have to ensure that consent obtained is valid. The GDPR requires that consent be freely given, specific, informed, and unambiguous in nature. How will that be done?

1. Plain language—Whatever form it takes, request for consent must be made in an intelligible and easily accessible form; the language used must be clear, plain and simple. Be careful not to use legalize language.

2. Separate—One must be able to clearly distinguish a request for consent from other matters.

3. Affirmative action—Consent obtained must reflect clear affirmative action (remember that you cannot have pre-ticked boxes; further, silence, lack of a response or inactivity on the part of a data subject cannot be considered as a valid consent).

4. Consent to all purposes[36]—Where processing personal data caters to multiple purposes, one must obtain separate consents for each of those purposes.

5. No detriment/disadvantage—Consent obtained in instances where the individual is unable to exercise genuine free choice or where there is

[35]ICO (n 14).
[36]Isabel Maria Lopes and Pedro Oliveira, _Evaluation of the Implementation of the General Data Protection Regulation in Health Clinics‘ (2018) Journal of Information Systems Engineering & Management 8.

disadvantage in refusing or withdrawing consent, such consent will not be considered valid.

6. No power imbalance—To the extent that there is unbalanced power relationship between the data controller and the individual, consent obtained may not be valid.

7. Not tied to contract–Where consent is considered as a condition to perform a contract (despite consent not being deemed necessary), it will be invalid.

8. Unbundled consent—Do not "bundle" consent. Where there are separate processing activities, the data subject must be able to consent (Note that where consent is revoked, you will have to stop processing personal data, as the consent is not considered valid.

9 Withdrawable—Data subject should be able to withdraw their consent at any given time (it should actually be easy for them to do so). To this effect, you must inform data subject of their right to revoke consent at the time of obtaining consent.

Note: Where consent is revoked, you will have to stop processing personal data, and will have to purge/delete such data, as there is no other legal justification for processing. This basically implies that you may have to significantly invest in processes/systems that would manage the consequences of consent withdrawal.

In instances where consent has been obtained before May 25, 2018[37], such, consent will be valid but only to the extent that it adheres to the new and more stringent requirements of the GDPR. Where the consent fails to match up to the expectations of the GDPR, a fresh consent may be obtained.

When it comes to direct marketing activities, one can only send direct marketing to someone by e-mail if they have consented to it, or you have an existing relationship with them and fall within the "similar products and services"

[37]Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, _The European Union General Data Protection Regulation: What It Is and What It Means‘ (2019) Information and Communications Technology Law 67.

exemption. Under the GDPR, obtaining consent to e-mail marketing is much harder. There might even be the case that supervisory authorities in Member States may bring in a "double opt-in" model which basically means that once the data subject has provided an initial consent, they must then send them another email which includes a link which they can click upon to validate the initial consent.

3.9.2 Consent—Additional Safeguards for Children

With regard to online services, you will only be able to get consent from a child where it is authorized by a parent. A child is defined as someone below the age of 16, and Member States can reduce this age to 13[38].

One can rely on the other processing conditions, but practically, it is almost impossible to explain a "legitimate interests" condition whilst processing a child's data. Please note, however, that when providing preventive or counselling services to a child, consent is not required.

The GDPR does not usually apply the "authorization from parent" restriction whilst obtaining consent from a child offline; however, considering how the GDPR treats consent, you'd be better off taking parental authorization[39].

There are other requirements as well that impact children. Privacy policies that are aimed at children must be extremely clear and simple. There is no way automated decision making and profiling can be directed or applied to children.

Additionally, the right to erase applies robustly and firmly to children. Note that Member State law may have additional restrictions in place with regard to processing of children‘s personal data[40].

3.10 Rights of Data Subjects

[38]Macenaite and Kosta (n 15).
[39]Marilyn Coleman and Lawrence Ganong, _Children‘s Online Privacy Protection Act‘, *The Social History of the American Family: An Encyclopedia* (2014).
[40]Robert Merrick and Suzanne Ryan, _Data Privacy Governance in the Age of GDPR‘ (2019) Risk Management 314.

One of the significant features of the GDPR has been the enhancement, strengthening, and extending of data subjects rights." This includes the following rights of access, right to rectification, right to ensure, right to restrict processing, right to object to processing, right to data portability. The response time for companies has been set forth as a month. There is an additional flexibility of increasing this time period by additional two months where request received are compounded.

In general, as per the GDPR, data subjects have the right to information (via notices), which means that data controllers and processors may be obliged to give data subjects information relating to the following[41]:

1. Contact details of the DPO (that is, if one is appointed);

2. The legal justification or basis behind processing of personal data;

3. Details about international data transfers;

4. Retention periods, or at least the parameters for determining a retention period; the right to object to data processing; the right to data portability; the right to withdraw consent;

5. The right to subject to data processing;

6. The right to data portability;

7. The right to withdraw consent;

8. The right to complain to supervisory authorities;

9. Whether the collection of data is a statutory requirement, or if it is required to enter into a contract;

10. Whether data subjects are required to give data, and if there are consequences of not giving the data;

[41]ibid.

11. If there is any automated decision-making, or profiling, the reasons for such processing, and the impact of such processing.

3.11 Subject Access Requests

Data subjects have the right to make a data subject access request (also referred to as DSAR or SAR)—this means that they have the right to seek confirmation from the data controller about the personal data that is being processed about them; they also have the right to ask for a copy of such personal data that the data controller holds about them[42]. By way of this right, data subjects can also ask for information about the sources where their data was collected from, how it is processed, and for what purposes it is being processed for, etc. Companies must provide this information free of any charge/cost to data subjects unless the request is either unfounded, or extremely cumbersome. If the data subject asks for more copies of the personal data, in which case you can charge a small fee. Historically, the exercise of this right has been seen as cumbersome and a fishing expedition (in the legal parlance, you may refer to it as a pre-litigation disclosure tactic).

If a SAR is made electronically (via e-mail), then the information sought should be shared electronically, unless a physical copy has been sought for. In fact, where possible, the data subject should be given secure remote access to their personal data. Companies have a month to respond to a SAR; this period can be extended up to 2 months if the SAR is a complex one, and/or the company is deluged with such requests.

Companies can withhold divulging personal data as a response to a SAR if such disclosure would "adversely affect the rights and freedoms of others". As per the Charter of Fundamental Rights, to be able to conduct business is a right. If we go by that, companies may be able to withhold IP, trade secrets, and other company confidential information by stating that disclosing such information would

[42]—Tobias Urban and others, _A Study on Subject Data Access in Online Advertising After the GDPR‘, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (2019).‖

adversely impact the right to conduct business[43]. As the dust settles in, we will have a better idea of how the exercise of this right will pan out.

In the past, companies have been able to circumvent and/or dilute DSARs by using the privilege card, or by stating that the requests were cumbersome, etc. However, if one were to look at current regulatory attitude towards enforcement of the GDPR and other data protection laws, it seems unsafe to use such strategies. Furthermore, considering that Member States can introduce exemptions, it is extremely unclear at this point whether regulators will take kindly to companies using such strategies.

Meanwhile here are a few quick tips on how companies can respond to SARs. Once you receive a SAR, you must first try and assess the exact nature of the request (what is it that the data subject wants?). You may also want to consider what personal data you store/process, or that personal data could be lying with third parties, or who will handle such requests within the company and ensure that a response is appropriate, or how the response will be provided for. Also, send an acknowledgment of receipt to the data subject making the request[44].

A SAR has to be evaluated properly to check that it is valid. A company should run a SAR past the DPO or a data privacy professional to comment upon its validity. If the SAR is found to be invalid, inform the data subject, and give them reasons why. If the request is found to be valid, you must initiate the process of data collection to respond to the request. If you feel that you need further identification proof, please request the data subject to provide such proof.

Once the data collection is initiated, ensure that you have all the personal data of the data subject required to respond adequately to the request—this is where the concept of data mapping and the requirement to maintain records of data processing come in handy. Once all this data is collected, it can be set forth in a

[43]Antonio Capodieci and Luca Mainetti, _Business Process Awareness to Support GDPR Compliance', *ACM International Conference Proceeding Series* (2019).
[44]—Alaa Altorbaq, Fredrik Blix and Stina Sorman, _Data Subject Rights in the Cloud: A Grounded Study on Data Protection Assurance in the Light of GDPR', *2017 12th International Conference for Internet Technology and Secured Transactions, ICITST 2017* (2018).‖

spreadsheet or a Word document and should be shared with the DPO[45] or a data privacy expert to review, During the review, if it is found that the company does not have the kind of' personal data that has been requested for, a communication should be sent to the data subject to that effect, along with a request that this be acknowledged. Ensure that any extra copies of this data that is shared with DPOs, and others, are deleted[46]. If you have the requisite data, you must respond to the data subject and attach the spreadsheet or the Word document that you have created.

Set forthwith is a simple flowchart that captures the aforementioned steps:

3.12 Right to Rectification

By exercising this right, data subjects can, without undue delay, get inaccurate personal data about themselves rectified[47]. Additionally, depending upon the purposes of processing, they can also have incomplete data completed.

If you have received a request to correct data, you must correct inaccurate data, or you must complete the information that is missing; additionally, you must cease processing until the data is corrected.

3.13 Right to Object

As per the GDPR, data subjects now have more enhanced rights in terms of objecting to data processing. In an instance where the legal justification of processing rests on public interest or where processing is by way of exercising official authority vested in the data controller, the data subject has the right to object to processing. Also, where legitimate business reasons are cited for processing, data subjects have the right to object. This includes having the right

[45]Danielle Bauer, _6 Steps to GDPR Implementation‘ (2018) Risk and Insurance Management Society, Inc. [46]Aurimas Šidlauskas, _The Role and Significance of the Data Protection Officer in the Organization‘ (2021) Socialiniai tyrimai 345.
[47]Michael Hintze, _Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR‘ (2018) SSRN Electronic Journal 776.

to object to profiling[48]. So, basically, this means that data subjects can object to processing based on legitimate interests, and to processing in the context of direct marketing, research, statistics, etc. Unlike under the DPD, the data subject no longer has to provide compelling legitimate grounds to object to data processing which was based on legitimate interests. In fact now, it is the data controller/processor that has to prove compelling reasons to process the data despite an objection made, which supersede the rights, freedoms, and interests of the data subject, or they have to prove that such processing is required to establish, exercise, or defend a legal claim[49].

Note that an individual can object to direct marketing at any time—this is an absolute right, and there are no exceptions.

> *Firms providing marketing services to other organizations need to double check whether they have valid consent from people to send marketing emails to them. Generic third-party consent[50]is not enough; companies will be fined if the break the law. ---Sieve Eckersiey (Director of Investigations at the UK ICO).*

In an instance where the data subject objects to direct marketing, you must immediately stop sending any marketing material to this individual, and if you are already processing their data, or such data is in your marketing databases, etc., you must immediately stop processing this data for marketing purposes. If you are even profiling for direct marketing purposes, you must immediately stop that.

Note that in terms of the restrictions on direct marketing, the GDPR needs to be read along with the e-privacy Directive (scheduled to become a regulation shortly) which has additional restrictions. If implemented, the new regulationwill

[48]Michèle Finck and Asia Biega, _Reviving Purpose Limitation and Data Minimisation in Personalisation, Profiling and Decision-Making Systems‘ (2021) SSRN Electronic Journal 675.
[49]Michael Hintze, _Automated Individual Decisions to Disclose Personal Data: Why GDPR Article 22 Should Not Apply‘ (2020) SSRN Electronic Journal 28.
[50]Sabina Daniela Axinte, Gabriel Petrică and Ioan Bacivarov, _GDPR Impact on Company Management and Processed Data‘ (2018) Quality - Access to Success 341.

replace the existing EU e-privacy and Electronic Communications Directive 2002, which was implemented in the UK in 2003.

3.14 Right to Restrict Processing

Data subjects have the right to get data processing restricted, in the following instances:

1. The data subject challenges the accuracy of personal data and the controller is in the midst of verifying whether the data is in fact accurate;

2. Processing of persona1 data is unlawful but the data subject exercises the right to restrict rather than ask to be forgotten;

3. The data controller does not need the personal data any longer for the reasons of processing per se, but needs it instead in the context of a legal claim; or

4. The data subject objects to the processing, and it is yet to be determined whether the data controller can continue to process data based on the "legitimate interests" ground.

When this right is exercised, or such a request is made, the data controller should not Process personal data, except with the data subject's consent; or for reasons of establishing, exercising or defending a legal claim; or for reasons of public interest. The data controller can, of course lift the restrictions, the data subject must be informed beforehand.

3.15 Right to Data Portability

This is one of the new features of the GDPR—the right to data portability. What it means is that if a data subject has provided their personal data to you, and you process that data through automated means, and such processing is based on consent or contract, then the data subject can exercise the right to request you to provide them with their personal data in a "structured, commonly used, machine-readable format", and where it is technically possible, to transmit such

data directly to another data controller[51]. Note that although data controllers should use formats (like CSV, XML, and JSON) that facilitate data portability, it is not a mandate that they should develop processing systems that are technically compatible.

3.16 Right to Erasure or Right to be Forgotten

Data subjects can have their personal data erased without undue delay by way of exercising this right. However, this is not an absolute right to the extent that data controllers can continue to process data instances where it is absolutely necessary in relation to the purpose the data was collected for, and where the data controller is not relying on consent as the basis for processing[52]. Additionally, a company can continue to process data for reasons of public interest or in the area, of public health, or where processing is for the reasons of historical research (in this case, the data controller must ensure that appropriate safeguards are place). Bear in mind that the exemption accorded to historical research is one where Member States can derogate.

As stated, this is not an absolute right. It only applies when:

- Data is no longer required.
- Consent has been withdrawn.
- Data subjects object to the use of the data and when their interests outweigh those of the company.
- Data was unlawfully collected/obtained.
- There is a legal obligation to delete the data.
- The data subject was a child when the data was obtained.

[51]Paul De Hert and others, _The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services‘ (2018) Computer Law and Security Review 776.
[52]Vincenzo Mangini, Irina Tal and Arghir Nicolae Moldovan, _An Empirical Study on the Impact of GDPR and Right to Be Forgotten - Organisations and Users Perspective‘, *ACM International Conference Proceeding Series* (2020).

A challenge which the companies may face whilst responding to a request related to erasing data that is in backup. It is not an easy task to search backfiles/spreadsheets. However, this right applies to data in production, backup archives. Companies must first secure their back-ups to prevent misuse of data.

Note that the GDPR is not applicable to anonymized data. Once the data in backups and archives is identified, these must be deleted. Additionally, where backups are concerned, the company must not make a processing decision affecting individuals[53]. It should mark/flag such data so that it is not misused, and consider additional layers of technology and security, whilst committing to permanent deletion if/when possible.

Once the request is received, the data controller must assess it to ensure that it is a valid request. As soon as possible, the controller should send an acknowledgement of receipt of the request to the data subject. To the extent that the request is deemed to be invalid, the controller should inform the data subject about it along with the reasons for such an assessment. If the request is deemed valid, the controller can ask for further identification, if required. Thereafter, the process of data collection must start. Once the personal data has been collected, all of it must be totally erased. The controller must then share the proof of deleted data with the DPO or with a privacy professional and seek counsel. Once this is approved, it can be shared with the data subject.

If there is no data found, then the data subject must be informed and his acknowledgement must be sought and received.

3.17 Automated Decision-making, Processing & Profiling

[53]Marko Milosavljević, Melita Poler and Rok Čeferin, _In the Name of the Right to Be Forgotten: New Legal and Policy Issues and Practices Regarding Unpublishing Requests in Slovenian Online News Media‘ (2020) Digital Journalism 43.

Data subjects have the right to object to any automated decisions that might have a direct legal or other significant impact on them. Such automated decision making includes those based on automated profiling, as well[54].

3.17.1 Profiling

The right to object to profiling is not a universal right. This right can be exercised only in certain circumstances. For example, when it comes to direct marketing purposes, data subjects have a broad right to object to any sort of automated profiling. You may ask what constitutes profiling. This could include in scope recruitment e-processes which do riot require any human intervention (where job applications and forms are completed via a website or an IT application, for example, SAP Success Factors, and were based on details completed, the application/form can get rejected by the website or the IT app in an automate manner, with no human intervention at all), the automated refusal of an own personal loan application on a bank's website, etc. It also includes instance like using cookies to trace individuals' activities on the worldwide web analyze or predict what they are likely to purchase or using geo-location technology to track movement of individuals.

The GDPR defines profiling as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular toanalyse or predict aspects relating to that natural person's performance at work, economic situation, health, personal preferences, interests, dependability, location, or movements.[55] Profiling per se, is not prohibited by the GDPR. However, there are restrictions. To the extent that any profiling is backed by a legal ground, and that it complies with the broader data protection principles as enshrined in the GDPR, it is allowed. The GDPR sets forth certain requirements for data controllers in terms of profiling[56].

[54]Adrián Palma Ortigosa, _Automated Decision-Making in the Gdpr. Algorithms in the Scope of the Data Protection‘ (2019) Revista General de Derecho Administrativo 23.
[55]Gil González and de Hert (n 23).
[56]Chiara Rustici, _GDPR Profiling and Business Practice‘ (2018) Computer Law Review International439.

- Controllers shall use appropriate mathematical and statistical processes when undertaking profiling[57].
- They must implement appropriate technical and organizational measures so that there is as less risk as possible, and in instances any risk or error occurs, these can be rectified[58].
- Personal data shall be made safe in a way that considers all potential risks to the data subjects' rights, and which prevents any sort of discrimination.

Data subjects can object to profiling which is necessary to perform a public interest task or is part of the official authority that vest in a data controller or is backed by legitimate interest grounds. But, in both these instances, a data controller can dismiss such objection if it can prove that the legitimate interest is compelling enough to overlook the data subject rights and freedoms, or if it can show that such profiling is imperative in terms of any legal claims.

What controllers need to pay special heed to is that they must clearly and explicitly inform data subjects (while first communicating with data subjects), via a privacy notice, that these data subjects have the right to object to profiling[59]. Companies must ensure that this part of the privacy notice is set forth clearly and separately from other parts of the privacy notice so that it catches the eye of data subjects. Additionally, whilst collecting personal data for profiling purposes, companies must inform all data subjects about the facts that the former are collecting data for the purposes of automated decision making and/or profiling. They must state the significance and the anticipated results of such profiling, and also the logic behind such profiling being carried out.

3.17.1.1 Decision-making based on Profiling

[57]Gil González and de Hert (n 23).
[58]Frederike Kaltheuner and Elettra Bietti, _Data Is Power: Towards Additional Guidance on Profiling and Automated Decision-Making in the GDPR' (2018) Journal of Information Rights, Policy and Practice 112.
[59]Gil González and de Hert (n 23).

We have stated earlier that profiling is permitted (subject to certain limitations and requirements being followed); however data subjects have the right not to be subjected to decision-making which is exclusively based on profiling or a similar automated data processing activity, which decision-making affects them legally and/or significantly. But, again, this is not an absolute right[60]. It is subject to certain exceptions. Companies can make decisions based exclusively on profiling, if the data subjects' explicit consent has been obtained, or if the decision is imperative toenter into a contract, or to perform a contract that is entered into between the company and the data subject; however, the company must ensure that it has implemented appropriate measures to secure data subjects' rights, freedoms, and legitimate interests. Companies can also engage in decision-making based on profiling if it is expressly allowed by EU law or any Member State law that the company subscribes to, and wherein said law sets forth appropriate measures to secure data subjects' rights, freedoms, and legitimate interests. This last exception is not something that companies can rely on, except rarely.

In practice, companies will most likely use consent as the basis for decision, making based on profiling. But whilst companies do so, they must be wary of the extremely stringent consent requirements[61]. They should ensure that all consent obtained is valid. To the extent that companies use the contract exception, they must bear in mind that this exception will apply where there is a pre-contractual relationship between the company and the data subject which sort of mandate the decision in question is.

Apart from ensuring that appropriate measures are in place to secure the data subjects rights, freedoms, and legitimate interests, companies must also inform data subjects adequately about all decision-making based on profiling, and also provide them with the following rights—

[60]European Union, Art. 22 GDPR - Automated individual decision-making, including profiling 2018.
[61]Eduardo Ustaran and Victoria Hordern, _Automated Decision-Making Under the GDPR – A Right for Individuals or A Prohibition for Controllers?‘ (*Hogan Lovells Chronicle of Data Protection*, 2017).

(i) right to have human intervention in place;

(ii) right to express their own point of view:

(iii) right to an explanation behind the relevant decision; and

(iv) right to challenge decision taken.

3.17.1.2 Privacy Notices or Fair Processing Information

Data subjects have the right to information. Well, the GDPR requirements for privacy notices must be one of the bigger dichotomies of the Regulation. While on the one hand it requires enterprises to make their privacy statements brief, straightforward, comprehensible, and readily available, on the other hand it forces companies to provide a vast amount of information about how personal data is being handled and other pertinent details.

So, here‘s how you address this dichotomy.

Consider layering for some weird reason, layering seems to remind you of the tiers of a multi-layered cake. Well, what you can do is that you can set forth in a short summary the purposes behind processing the data and give that to the data subjects, whilst setting out links where data subjects can read the entire notice in detail if they prefer to get details. Let's just admit that most people will not read detailed privacy notices. So, layering helps kills two birds, it sets forth all that a company is going to do with a data subject's personal data, and yet stops short of killing people with information.

For specific instances, consider using additional notices—here's an example. Say, one of your customers wants to do a holiday promotional campaign for its products, and offers attractive discounts to its partners' employees, etc. What you have to do is to provide a link to your employees which takes them to your customer' website/webpage where they might have to enter their personal data (names, email addresses, etc.) in order to avail of the discount. So, here, you can draft a short privacy notice for your employees stating the background and purpose of the promotion, and then informing them that any personal data would

be used by the customer (a third party) in order to facilitate the discounts, etc., and that processing of data would be as per the third party's privacy policy, and that you cannot assume responsibility of the security of personal data given by the employees to the third party on their own accord, and of such data lying in third party' systems.

Avoid legal language and jargon—this is an occupational hazard if lawyers are drafting your privacy notices. However, you must bear in mind that the layman will most likely not be able to make sense of words like "processing‖, "controller", etc., unless these terms are broken down into plain and simple language and instances that make sense to them. If you are putting up a notice on your website, why not try and use a short video, an animation, or a cartoon about how you process personal data rather than put up a lengthy notice?

3.17.1.3 Instances and Exemptions

As for the timing of privacy notices, these must be provided to data subjects when you collect the personal data from them. However, if you are collecting personal data from a third party, or if you are going to disclose personal data to a third party, you must inform the data subject within a reasonable time-period, but not more than a month after, it was collected. To the extent that this personal day that you obtained from a third party is used to communicate with the data subject themselves, you must inform the data subject when you first communicate with them. And, if personal data is disclosed to a third party, inform data subjects immediately.

However, in certain instances, when you get data from a third party, you may, be required to give notice to data subjects." These instances are set forth here

(1) if the data subject already has the information;

(2) if the information to be provided is going to be a cumbersome task (consider where research, or for statistical purposes, etc.);

(3) where obtaining of data from a third party is per EU or Member State law, and there are appropriate security measures in place;

(4) where such information is guarded by reasons of professional secrecy.

When you decide to use obtained personal data for a new purpose, you must provide a privacy notice to data subjects, prior to processing.

3.18 Privacy Notices--Form & Content

In keeping with stricter transparency requirements of the GDPR, privacy notices are an imperative[62]. Companies must provide valid privacy notices to data subjects that inform the latter of the manner in, and the purposes for, which their personal data will be processed. In addition to being short, straightforward, understandable, and readily available (as we saw in Consent), such notifications will also need to fulfil the stricter GDPR criteria (which have been listed in the paragraph below). This essentially necessitates the revision of current privacy notifications, and in certain cases, the creation of new privacy notices.

No matter whether you obtain personal data directly from the data subject, or whether you choose to use a third party for that purpose, you must include the following information on your privacy notice[63]:

- Identification and contact information for the data controller. If the data controller has a representative, add the name and contact information of this person or organisation.
- Name and contact information for the data protection officer of the data controller (DPO)
- The objectives of data processing.
- The legal justification or basis of processing.

[62]Kirsten Martin, _Do Privacy Notices Matter? Comparing the Impact of Violating Formal Privacy Notices and Informal Privacy Norms on Consumer Trust Online‘ (2016) Journal of Legal Studies 378.
[63]Andrew Denley, Mark Foulsham and Brian Hitchen, _Privacy Notice(S)‘, *GDPR – How to Achieve and Maintain Compliance* (2019).

- To the extent that legitimate business interests are the lawful basis of processing, include these interests on the privacy notice.
- To the extent that consent is your lawful basis for processing, include the right of the data subject to withdraw consent.
- Where you collect data via a third party, include the categories of personal data processed.
- Where you outsource or use vendors or other third parties for processing personal data, include the vendor details (recipients of personal data).
- If data is obtained from a third party, and not from the data subject, then include details of the source of such personal data (include the use of a public source too).
- For any actual and/or intended transfer of data outside of the EU include details of such transfer, and of the safeguards used.
- Retention period of personal data, and the criteria used to calculate tha retention period (statutory, tax purposes, others).
- Includes details about data subjects' rights. This should also have details about the right to complain to a supervisory authority.
- To the extent that you carry out any automated decision making (including profiling), include details.

3.19 Accountability

Right when you were thinking that it is enough that you comply with the six (6) data protection principles and with the processing conditions, it seems like this is

not going to be enough. The GDPR requires that you are able to show that you are complying[64].

The GDPR introduces concepts of accountability, privacy by design and by default, data privacy impact assessments, etc. These will enable supervisory authorities to dig deep into a company's processes in order to verify whether they are actually complying with the requirements. What it means for companies is that they cannot anymore think of privacy as a mere sidenote or a reference point; privacy needs to be embedded into a company's systems and processes— they need to be breathing and living privacy.

3.20 Data Mapping

You must have heard of the gold rush in America (specifically in and around, Colorado) way back in the 1850s and thereafter. Scenes of "Mackenna's Gold" (starring Gregory Peck and Omar Sharif) play in your head—early prospectors, explorers, etc., "mapping" their way to Colorado, to the Grand Canyon, drawn in by the tales of rivers flowing with gold. Somehow, when you look at how the concept of personal data has evolved over the last few decades and looking at the role that smart use of personal data plays in boosting business profitability, you could think of personal data as the new gold.

Just like the physical map played an important part during the "gold rush" plays, in modern times, in order to use personal data smartly, companies need to invest in data mapping which is basically all about recognizing, locating, deciphering, and charting out the personal data flows within the company[65].

What exactly is data mapping, you might ask. If we are still using "gold rush‖ metaphors, think of Gregory Peck and Omar Sharif (rather, their respective characters) trying to one-up each other in their search for gold, fighting over torn map in order to chart the area around the Grand Canyon and the Colorado river,

[64]European Commission (n 12).
[65]Alexia Dini Kounoudes and Georgia M Kapitsaki, _A Mapping of IoT User-Centric Privacy Preserving Approaches to the GDPR‘ (2020) Internet of Things.

decoding what the map states about following the rising sun's shadow all that jazz. Sounds complicated? Well, it isn't, not really[66]. Thankfully, one does not need to follow the sun's shadow to anywhere in this case. However, one does need to chart out the 5Ws of personal data, as they are popularly referred to. Those would be—WHO, WHERE, WHAT, WHEN, AND WHY. Let's try simplify these, shall we?

WHO—Who are the data subjects? Who are the data controllers? Who are the data processors?

WHERE—Where is the data located? Transferred to locations outside the EU.

WHAT—What personal data is being collected? What's the purpose behind collecting and processing such personal data?

WHEN—How long will the personal data be retained? When will it be deleted, destroyed?

WHY—Why do you need to process the data? Why do you need to keep this data after the purpose has been served?

Data mapping is not a GDPR requirement per se; however, it does help the organization is complying with its various other GDPR, and other applicable personal data protection statutory/regulatory obligations. Additionally, it can assist in using personal data in a smart manner in order to derive operational benefits. From a GDPR compliance perspective, data mapping helps data controllers and processors to maintain detailed records of their data processing activities, to be made available to Supervisory Authorities on request. It also caters to the accountability requirement of the GDPR. Furthermore, it helps in meeting the Privacy by Design and by Default requirements[67].

[66]Ellen Poplavska and others, _From Prescription to Description: Mapping the GDPR to a Privacy Policy Corpus Annotation Scheme', *Frontiers in Artificial Intelligence and Applications* (2020).
[67]Ke and Sudhir (n 19).

Apart from helping a company meet statutory obligations, data mapping assists in a myriad of other ways.

- By way of identifying business processes and IT systems that deal with personal data, and by conducting adequate privacy risk assessments impact assessments of such processes and systems, companies are to figure out if system efficiencies can be improved, and data flows can be managed more efficiently.
- Companies can also determine how data can be used in smarter ways, whilst adhering to controls and limitations, as prescribed by the law.
- Companies, while mapping data, are able to assess the risks of data breach (via appropriate risk and impact assessments), and are, therefore, able to foresee unpleasant situations so that they can take appropriate a risk mitigation measures. In this way, a company can mitigate both reputational as well as financial loss.
- A data map can help a company respond effectively to data subjects' requests. In a pre-litigation or litigation scenario, it assists in responding to discovery requests, and, therefore, minimizes related costs.
- It helps comply with various other statutory record retention requirements, etc.

3.21 Maintaining Data Protection Registers

In keeping with the data mapping activity described previously, the companies will need to keep records of processing. Although the GDPR does do away with the need to notify local supervisory authorities about data processing activities, companies still have the responsibility to maintain detailed records of all data processing activities (and be able to showcase them to the supervisory authority if they come visiting).

In terms of the content of these registers, Member States set forth varying obligations—in the UK, it would be sufficient to have brief summaries while, in France, a company might be required to keep extremely detailed information.

Good news is that small companies (employing less than 250 employees) need not do this unless they engage in high-risk processing, frequent processing, or processing of data that is sensitive.

Most organizations are finding it tough to wrap their heads around this requirement. We saw a passing reference to it in the Data Mapping section earlier. From the periphery, it does appear quite tough and onerous. These records have to be maintained so that they can be provided to the supervisory authority on request. When you think of legacy data, this requirement seems particularly cumbersome, and it probably is. To configure old systems to maintain records of all personal data within an organization is quite exacting; however, the great news is that there are several new and innovative technical solutions available in the market currently that can help organizations in building and maintaining their data maps (or, data inventories), and data protection registers (DPRs) or the records.

3.22 Data Controller—Data Processing Register Obligations

Data controllers will be required to maintain DPRs which must include the following information[68]:

- The name and contact information of the controller, the names and contact information of any joint controllers (where applicable), and the names and contact information of the controller's representatives or data protection officers.
- The reasons for data processing.

[68]Shakila Bu-Pasha, The Controller‘s Role in Determining High Risk and Data Protection Impact Assessment (DPIA) in Developing "Digital Smart City‘ (2020) Information and Communications Technology Law 771.

- Descriptions of the types of data subjects and personally identifiable information.
- Descriptions of types of receivers of personal data (including third parties in foreign countries and/or international organisations).
- Details of personal data transfers to foreign nations.
- —Retention periods‖ for different categories of personal data.
- General description of the security measures in place. companies would be required to answer the following questions:

1. What personal data companies have got/collected? (Name, telephone number, address, date of birth, etc.)

2. Why do the companies have the personal data? (Legal basis for processing)

3. Where or with whom do companies share the personal data (Internally? Externally? or Both?)

4. How do you share the personal data in a protected manner? (Data transfers/safe data transfer mechanisms)

5. For how long is the personal data retained? (Retention policies)

6. When and how do companies delete/destroy data? (Consider both hard and electronic copies)

7. How do companies ensure security of the personal data? How do companies ensure that the security controls in place are effective?

3.23 Data Processors—Data Processing Registers Obligations

Data processors would be required to maintain the following information[69]:

[69]Yordanka Ivanova, _Data Controller, Processor or a Joint Controller: Towards Reaching GDPR Compliance in the Data and Technology Driven World‘ (2020) SSRN Electronic Journal 109.

1. Name and contact details of the processor, any representatives (where applicable), and the name and contact of the appointed DPO;

2. The name and contact details of the data controller, their representatives (where applicable), and their DP0s.

3. The categories of data processing that the processor carries out for the controller.

4. Details of any international transfer of personal data (outside of the EU)

5. Details of security controls in place to keep the data safe and secure.

3.24 Data Privacy Impact Assessments

The GDPR requires that companies that engage in any "high risk" projects and/or processing activities must conduct data privacy impact assessments (DPIAs). In any case, by way of the previous DPD, several companies were conducting such PTAs for technology that they used for processing of personal data. Here are a few things that you must consider in terms of conducting DPIAs.

First and foremost, consider whether the processing can be seen as ―high risk.‖ The GDPR provides some guidance on this point and sets forth some examples such as artificial intelligence, smart technologies (including wearables), credit checks, social media networks, workplace access systems/ identity verification.

DNA testing etc. Where a DPIA is required, companies must seek advice from the DPO or a privacy professional. In instances, where a DPIA is conducted, and it seems that the remediation measures in place are not sufficient in relation to the risks, then companies must consult the local supervisory authority and seek advice. Please note that any such consultation would require time – supervisory

authorities have upto 14 weeks to consider your application for a consultation and can even extend this time[70].

3.25 Data Protection Officers

We had mentioned "beat cops" before. Depending upon the data processing that you carry out, you may be obliged to appoint a beat cop, or a data protection officer (DPO). Cannot terminate the services of your DPO for doing their job, and your DPO must be reporting to the highest-management levels in the company.

The DPO is a very important element of the "accountability" framework that we discussed before. DPOs are mandated by Member States like Germany[71].

If required to do so by the legislation of your Member State, you must designate a DPO if you are a public entity (except for courts acting in their judicial capacity), if your core processing activities are about large scale, regular and systematic monitoring of data subjects, or if you are processing sensitive data on a large scale (such data includes information about criminal offenses).

The obligation to appoint a beat cop (or DPO) rests on both data controllers and processors. Even if you are not mandated to do so, it is just a good idea to voluntarily appoint a DPO, as they add significant value to your privacy compliance program and are also your representative before a supervisory authority. However, note that even with a voluntary appointment, all other GDPR provisions with regard to a DPO will kick in (including shelter from dismissal). To avoid this, be careful of the title you offer to the DPO, and the job description and scope of their activities.

A group of companies may want to have a single DPO, but they must ensure that this individual is easily accessible to all units of the group, and that they are a

[70]Dimitra Georgiou and Costas Lambrinoudakis, _Data Protection Impact Assessment (DPIA) for Cloud-Based Health Organizations‘ (2021) Future Internet9.
[71]Minjung Park, Sangmi Chai and Myoungjun Lee, _A Study on the Establishment of Data Protection Officer(DPO) Position under GDPR Enactment‘ (2018) The Journal of Korean Institute of Communications and Information Sciences 117.

subject matter expert in all matters related to data privacy. However, this might be a problem if the DPO does not speak the language of a particular jurisdiction where there are several data subjects, or if the DPO does not reside in, or is not familiar with the requirements of a particular Member State where one of the group companies might operate in. In such cases, you may want to have a group DPO, and then appoint several other data privacy experts/leaders in other group entities and jurisdictions that report to this group DPO.

3.26 Roles & Responsibilities and Qualifications of a DPO

The basic responsibilities of a DPO are to monitor and supervise whether you are complying with the GDPR, to inform and advise you, and to liaise with supervisory authorities. They should be able to operate independently and must have access to all resources that they need to comply with the GDPR. A DPO can also have other roles within the company if there is no conflict of interest— for example, they cannot be a CISO, or an HR head, or part of the Compliance team, as that would mean marking their own homework[72].

There is no mandatory qualification that a DPO must have—it is good to have relevant certifications, like CIPP[73], etc., but the lack of such certifications is not a deal-breaker. If the DPO has subject matter expertise when it comes to data Privacy regulations, implementation, and practice, it isgood enough. The WP29 has defined certain minimum requirements when it comes to acumen of a DPO[74]:

- The DPO is expected to be an expert in building and implementing effective data privacy programs.

[72]ibid.
[73]Timothy Banks, _GDPR Matchup: Canada‘s Personal Information Protection and Electronic Documents Act‘ (2017) The International Association of Privacy Professionals.
[74]Marija Boban, _Protection of Personal Data and Public and Private Sector Provisions in the Implementation of the General Eu Directive on Personal Data (GDPR)‘ (2018) 27th International Scientific Conference on Economic and Social Development.

- The DPOs need not be lawyers, but they should possess in-depth knowledge of applicable data privacy legislation, and how to put statutory requirements into practice.
- Certifications like CIPP, CIPM[75], are not mandatory, but good to have.
- The DPO should possess deep knowledge of IT security, infrastructures etc.
- To top it all, the DPO must be able to demonstrate the highest levels of integrity and ethics and be able to thus comply with the GPDR.

3.27 Privacy by Design and by Default

To start with, Privacy by Design and by Default requirements of the GDPR apply only to data controllers, and not to data processors. Although the concepts of Privacy by Design and by Default have been thrown around in conversations, and have been discussed in boardrooms, and have been a mainstay of data privacy discussions all around the world, these requirements have rarely been legislated except for countries such as Canada and Australia. That is, until now. The GDPR requires companies to now implement this approach, especially while creating databases, systems, technologies, infrastructure, etc. What it means is that companies will now have to focus on privacy upfront (and not treat it as a footnote) and right at the beginning and embed privacy into the very architecture of its processes and systems. Data protection cannot be mere lip-service anymore.

Whenever a company is undertaking a new activity involving processing of personal data or is implementing a modified or new system that processes personal data, the GDPR requires the company to consider the approach of

[75]Banks (n 73).

Privacy by Design[76]. The company must, thus, take appropriate steps to ensure compliance with data privacy principles, and safeguard their processing whilst meeting data privacy requirements and protecting data subjects' rights, both while deciding upon the means of processing and while the processing is happening. This would include considering the idea of limiting the processing of data and/or data minimization. While considering Privacy by Design, the company must look at the following: kind of technology used (should be state of the art preferably), cost of implementation of such technology, the nature, scope, purposes, etc. of the processing activity, risks to data subjects, etc.

The GDPR also requires data controllers to implement Privacy by Default—it is a follow-up to Privacy by Design, and it ensures that personal data is not, by default, made available or accessible to multiple and/or unauthorized users. For example, profiles on a website should not, by default, be set up as "public". It means that only personal data which is identified as being absolutely necessary for specific processing purposes is processed, by default.

3.28 International Data Transfers

Transfer of personal data outside of the EU is prohibited under the GDPR regime, unless certain conditions are fulfilled. There are some minor exemptions to this. Although the broader provisions remain the same as in the DPD, there are some significant changes. For example, consent for data transfer must be explicit, and is subject to several other limitations[77]. Unlike before, the use of Model Contract Clauses does not need authorization by a supervisory authority; however, they may still want to be informed about the use of these clauses. Further, the Binding Corporate Rules now have statutory backing behind them[78]. There is also a push for data controllers and data processors to follow codes of conduct or have certifications in place to be considered adequately safe in terms

[76]Harald Gjermundrød, Ioanna Dionysiou and Kyriakos Costa, _Privacytracker: A Privacy-by-Design GDPR- Compliant Framework with Verifiable Data Traceability Controls', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (2016).
[77]Tran (n 21).
[78]Zuzanna Gulczyńska, _ A Certain Standard of Protection for International Transfers of Personal Data under the GDPR ' (2021) International Data Privacy Law 11.

of data transfers. Transfers can be prohibited due to public interest or under EU or Member State law—the prohibition does not apply to transfer to adequately safe jurisdictions but applies to transfers made based on Model Contract Clauses.

One of the biggest challenges regarding cross-border transfers arises in the instance of onward transfers of data. The extension of data transfer restrictions to onward transfers has rendered things to be quite complicated. How does one decide liability if there is an onward transfer that breaches the GDPR? Will the initial exporter be liable considering that in most cases the importer may not be subject to the GDPR? But then that would be unfair as the initial exporter has limited control over the importer (especially where the importer acts as a controller)[79].

There is a minor exemption in place for cross-border transfers[80], especially in instances where an employee travels abroad and carries their laptop with them, or where an employee emails a person who happens to be outside of the EU. The minor exemption applies where no other basis for cross-border transfer can be used, where the transfer is not repetitive in nature, where only very few data subjects are impacted, where there is a compelling business interest that does not supersede the rights and interests of data subjects, where risks have been assessed and appropriate safety controls have been put in place, and where data subjects and supervisory authorities have been notified about the transfer[81].

Keeping the above in mind, it seems quite implausible that the minor transfer exemption will come into play. It is not feasible that a company will notify data subjects each time an employee decides to take a vacation abroad and takes his laptop with him, or to notify supervisory authorities if an employee sends an email to someone sitting in a foreign country.

[79]Martina Mantovani, _Contractual Obligations as a Tool for International Transfers of Personal Data under the GDPR‘ (2020) SSRN Electronic Journal 32.
[80]Danny S Guaman, Jose M Del Alamo and Julio C Caiza, _GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Apps‘ (2021) IEEE Access 203.
[81]Itziar Sobrino García, _The Adequacy Decisions in Cross-Border Data Transfers. The Case of Data Flow between the European Union and the United States‘ (2021) Revista de Derecho Comunitario Europeo 21.

Also, what does a data controller do if faced with requests for personal information coming from foreign regulators? How do they balance data protection obligations with the risk of being sanctioned by foreign regulators and/or courts? The GDPR states that for a national/local court to consider any foreign disclosure request, such request has to be made under an appropriate treaty. Also, again, cross-border transfer on account of foreign disclosure requests is allowed where there is public interest at play, or where it is on account of legal claims.

3.29 Data Security Breach Notification

Data controllers are obligated to notify the supervisory authority in case of a personal data breach, and in some instances, may also be required to inform data subjects[82]. Data breach notification rules are not a new concept—they have been around for years specifically for telecom providers globally, and in almost states across all sectors in the US.

A personal data breach happens when a security breach leads to the unintentional or illegal destruction, loss, modification, disclosure, or access to personal data.[83].The GDPR applies only to actual, and not to potential, breaches.

The first thing to do when a breach occurs is to assess if it is going to pose a risk to data subjects. If there is a finding of no risk, or very minor risk, then you may not need to notify the supervisory authority. But you will still have to maintain records of the data breach.

If there is a finding of risk to data subjects, you must notify the supervisory authority as soon as possible, and definitely within 72 hours from when you know of the breach. This notification must include everything that you know about the breach (this 'information can be provided in stages if not available immediately). If a breach poses high risk to individuals, then the affected data

[82]Maria Karyda and Lilian Mitrou, _Data Breach Notification: Issues and Challenges for Security Management‘ (2016) Mediterranean Conference on Information Systems (MCIS) 9.
[83]Chlotia Garrison and Clovia Hamilton, _A Comparative Analysis of the EU GDPR to the US‘s Breach Notifications‘ (2019) Information and Communications Technology Law 67.

subjects need to be informed as well. Such notification must be made immediately and must be detailed. If communicating directly with data subjects proves to be cumbersome, then companies can use alternative methods such as newspaper releases, etc. Note that if the personal data that is breached was encrypted or if there were appropriate technical and physical safety mechanisms/controls in place, then a breach will not be considered high risk. If there is no high risk, then no further notification is required, and you can close the process after all internal action plans have been completed.

3.30 Data Processor Obligations

Under the older DPD, data processors had the safety net of the data controllers. However, this safety net has quite literally been taken away under the GDPR. The GDPR, in fact, imposes data protection requirements directly on data processors, and will hold them directly liable for non-adherence[84].

Here's a bird's eye view of the main obligations that have been imposed directly upon data processors. These obligations have been articulated in Article 28 of the GDPR.

- Implementing suitable technological and organisational safeguards to protect personal information.
- Maintaining detailed records of all data processing activities.
- Appointing a data protection officer, as required in certain instances of data processing, and appointing a representative that is in the EU in a situation where the processor is based/located outside of the EU.
- Adhering to cross-border transfer requirements/mechanisms.
- Informing data controllers of data privacy breaches.

[84]Jenna Lindqvist, _New Challenges to Personal Data Processing Agreements: Is the GDPR Fit to Deal with Contract, Accountability and Liability in a World of the Internet of Things?' (2018) International Journal of Law and Information Technology 211.

I have made a deeper foray into these data processor obligations in the following sections. In this section we will take a cursory look at how these obligations will impact data processors, data processing agreements, relationship between data controllers and data processors, etc.

The definitions of data controllers and data processors remain largely the same under the DPD and the GDPR. A processor is a natural or legal person, public authority, agency, or other entity that processes personal data on behalf of a controller. A controller has been defined as the natural or legal person, public authority, agency, or other body that alone or jointly with others determines the purposes and means of processing personal data; where the purposes and means of processing are determined by EU or Member State laws, the controller (or the criteria for designating the controller) may be designated by those laws.

One major aspect that has been brought to the forefront by the GDPR is the level of enforcement against data processors. Now, more than ever, we will see how Supervisory Authorities (SAs) will have direct enforcement powers against data processors. SAs can now, whilst executing their investigating powers, directly seek information from data processors, or ask them for access into the latter's premises or to the personal data. SAs can also put to use their corrective powers, issue cautionary notices and/or admonition, or just demand that data processors comply with the GDPR. And let's not forget the significant administrative fines that could be levied (€20 million, or up to 4% of the annual turnover)[85] (details are provided in the section on Enforcement and Sanctions).

While earlier, the DPD was not extremely comprehensive about the entire process of deciding upon processors (and, sub-processors), the GDPR ups the game quite a bit, and is extremely prescriptive about this topic.

3.31 Choosing the right processor

[85]Paul Voigt and Axel von dem Bussche, _Enforcement and Fines Under the GDPR‘, *The EU General Data Protection Regulation (GDPR)* (2017).

Whilst choosing a data processor, the data controller should consider someone that can give sufficient guarantees about the implementation of adequate technical and organizational measures per Article 32 of the GDPR[86]. This can be quite a challenge for data controllers—the due diligence which is required, and, therefore, if data processors adhere to an approved code of conduct' or have a certification (such as ISO 27001, ISO 27002, ISO 18028, SSAE 16 etc.)[87]in place, such data processors will score brownie points when it comes to controllers choosing data processors.

3.32 Having a Data Processing Agreement (DPA) in place

Once a data processor is selected, the controller and the processor should enter into a DPA which sets forth the subject matter of data processing, the nature, the purposes, duration, data subject categories, personal data types, rights and obligations of the data controller, etc.

What a DPA does primarily is that it obligates data processors to do the following:

1. Process personal data only as per the instructions of the data controller (such instructions shall be documented). Where such processing relates to data transfers outside of the EU and is required by the Union or the Member State law where the data processor is, the data processor shall inform the data controller of any legal requirement, unless it is prohibited to do so by way of public interest[88].

2. Ensure that its employees, contractors, representatives, etc., that are processing the data or are authorized to process the data have signed on to appropriate data protection and confidentiality obligations (this basically entails having signed NDAs in place).

[86]Catherine Barrett, _Emerging Trends From The First Year Of EU GDPR Enforcement‘ (2020)*The SciTech Lawyer*. [87]Eric Lachaud, _ISO/IEC 27701 Standard: Threats and Opportunities for GDPR Certification‘ (2020) European Data Protection Law Review 546.
[88]Fabian Simon Frielitz and others, The Contract Data Processing Contract (DP Contract): Relevance and Practical Significance for Diabetology‘ (2020) Diabetologie und Stoffwechsel 77.

3. Take adequate and applicable security measures to protect the personal data.

4. Take prior consent from the data controller before engaging sub-processors, and have such sub-processors sign on to similar DPAs[89].

5. Help data controllers in responding to data subjects' requests.

6. Help data controllers in complying with obligations relating to data security, data breach notifications, privacy impact assessments, etc.

7. Ensure that personal data is either deleted, shredded, and/or returned, depending on what the data controller wants, once the project or the engagement is over, and delete any existing copies, unless there is a legal requirement to retain such data.

8. Cooperate with the data controller in providing whatever information is required to demonstrate compliance with data processor obligations, and assist data controller in audits, inspections conducted by the controller or its representatives.

3.33 Sub-processing

If the data processor chooses to subcontract, then the following should be kept in mind[90]:

1. When engaging a subcontractor or a sub-processor, the data processor must obtain prior consent from the data controller (such consent has to be written or documented and can be general or specific). If a general consent has been obtained, then in every instance where the data processor wants to change or add sub-processors, it must inform the data controller, and check whether there is an objection.

[89]ibid.
[90]Cyber GRX, _6 Security Controls You Need For General Data Protection Regulation (GDPR)‘ (*Product Resources*, 2018).

2. When subcontracting, the data processor must pass on all obligations imposed by the data controller to the sub-processor by way of a DPA.

3. The data processor is liable to the data controller for the performance of the sub-processor's obligations in the event of failure on the part of the sub- processor to perform its obligations.

3.34 Increased liability

In the current GDPR regime, data controllers continue to remain liable for any damage that is caused by processing which is non-compliant with the GDPR. Data processors, on the other hand, are only liable for damage caused by any processing to the extent that they fail to comply with data processing obligations under the GDPR, or, if they act outside of the ambit of the data controller's instructions. However, this is a significant shift from the DPD where data processors were not directly liable to data subjects for damage caused by processing.

For both, data controllers and data processors, there is exemption from liability if they can demonstrate they did not cause the alleged damage. Additionally, they can be held jointly liable for damage caused by any processing that they do together.

3.35 The Security Principle

As per the GDPR, data controllers and data processors shall process data in a safe and secure manner whilst using "appropriate technical and organizational measures"[91]. This, basically, implies that they must consider aspects like a privacy risk analysis, policies and processes, and physical and technical measures to ensure safety of processing of data. Controllers must ensure that their processors also take into account security of personal data (by way of data processing agreements, etc.). Security measures, whilst taking into account state

[91]Antoni Gobeo, Connor Fowler and William J Buchanan, _5 Data Protection by Design and Default‘, *GDPR and Cyber Security for Business Information Systems* (2020).

of the art, and the cost aspects, must also be associated closely with the types of processing and the underlying risks. Controllers and processors should consider options such as pseudonymization and anonymization[92]. All measures taken should ensure "confidentiality, integrity, and availability"[93] of systems and services that include processing of personal data. Aspects such as data recovery, disaster recovery, etc., have to be taken care of. Controllers and processors should also consider aspects such as vulnerability assessments, penetration testing, privacy risk assessments, etc.

3.36 The GDPR Sanctions Regime

When it comes to punishments, the GDPR provides consequences that leave everyone stunned. Under the GDPR, supervisory agencies may impose penalties of up to €20 million or 4% of the prior fiscal year's global annual revenue, whichever is greater. And if you believed they would stop there, you are incorrect. The government has the authority to give warnings and may audit you at any moment. They may even temporarily halt your processing operations. Data subjects may individually sue you for damages recompense (material damage, as well as for the distress caused). You may also be sued by non-profit organisations representing data subjects.

The larger fine of €20 million or 4% of the total worldwide annual turnover of a business in the preceding financial year applies to non-compliance to provisions such as failure to comply with the 6 general data protection principles, or for carrying out processing without meeting at least one processing condition. The lesser penalty of 2% of a company's annual turnover or €10 million applies to non-compliance like failing to notify a data breach, or failure to put together an adequate contract with a data processor.

[92]Peter Štarchoň and Tomáš Pikulík, _GDPR Principles in Data Protection Encourage Pseudonymization through Most Popular and Full-Personalized Devices - Mobile Phones‘, *Procedia Computer Science* (2019).
[93]Jan Zibuschka and others, _Anonymization Is Dead - Long Live Privacy‘, *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI)* (2019).

While determining appropriate sanctions for non-compliance, the supervisory authorities are likely to look at several things, including the nature and seriousness of non-compliance, whether there was negligence or malefic intent, what steps were taken to remediate the breach, any financial benefits derived from the breach, whether the company cooperated with the supervisory authority in any investigations, audits, etc.

3.37 Data Ownership

3.37.1 What do we mean by Data Ownership?

The rapid expansion of the digital world has led to questions being raised regarding the ownership of data—who "owns" data? When I provide my data to a third party, am I handing over "ownership" of that data?[94] This also brings into play an interesting question on the intellectual property rights associated with the data—who is the copyright holder of the data?[95]

Data ownership means owning and having legal rights and complete control over data—whether as a single piece or as a set of elements. It is interesting to note that the GDPR, which is focused on the protection of an individual's rights to their personal data, does not make any reference to the term "data ownership". An individual whose data is being processed, is not referred to as a "data owner". Instead, terms such as "data subject" and "data controller"[96] are used. India's draft legislation on privacy also does not contain any references to the terms "data owner" or "data ownership"[97] and instead uses terms such as "data

[94]Christian Janßen, _Towards a System for Data Transparency to Support Data Subjects‘, *Lecture Notes in Business Information Processing* (2019).
[95]Udo Milkau, _The GDPR: Halfway between Consumer Protection and Data Ownership Rights.‘ [2018] Journal of Digital Banking.
[96]Ivanova (n 96).
[97]Milkau (n 136).

principal" and "data fiduciary"[98]. So, the question that can then be asked is does the law not safeguard my interests as a data owner?[99]

3.38 Legal Data Ownership

In this context, it is interesting to read the provision of the GDPR which deals with data portability and the right to be forgotten. Under Article 20 of the GDPR[100], the data subject has the "right to receive personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used, and machine-readable format and to transmit those data to another controller without hindrance from the controller to which the personal data were provided, where the processing is based on consent and has been carried out by automated means.

Individuals have the right to have their personal information directly communicated from one controller to another (if technically feasible). Coupled with the GDPR's right of erasure and right to be forgotten, this essentially means that an EU citizen can move his personal data from one supplier of services (such as platforms hosting playlists, social networks, etc.) to another and request the original supplier to delete (subject to legal requirements) all references to his
/ her personal data. In fact, the individual is now, for the very first time, the proprietor of his or her own personal information.

This shift in ownership of personal data could have far-reaching repercussions with leverage on the side of the person owning data. I could seek discounts with my grocery store in exchange for retaining my personal data with them; threaten to shift my personal data if I have had a terrible interaction with a company; participate in a social media program boycotting certain organizations for their

[98]—Julia M Puaschunder, _Data Fiduciary in Order to Alleviate Principal-Agent Problems in the Artificial Big Data Age‘ [2019] SSRN Electronic Journal.‖
[99]Julia M Puaschunder, _Data Fiduciary in Order to Alleviate Principal–Agent Problems in the Artificial Big Data Age‘, *Information for Efficient Decision Making* (2020).
[100]—Ralph O‘Brien, _Privacy and Security: The New European Data Protection Regulation and It‘s Data Breach Notification Requirements‘ [2016] Business Information Review.‖

perceived abuses.' Since predictions are that data is the next liquid gold, I could sell my data to the highest bidder as well.

3.39 Legal Data Ownership vs. Assignment of Data Ownership

What we have dealt with above is the legal ownership of personal data. However, who 'owns' the data within an organization to whom the data subject has entrusted his / her personal data, is a question that also needs answering. Take for instance, the banking sector. An individual may have submitted her personal data for the purpose of opening a bank account. But there are other departments as well—housing finance, car financing, investment advisory etc. So, who then takes stewardship of that personal data?

This brings in the concept of 'enterprise data. According to The Data Governance Institute, enterprise data doesn‘t —belong‖ to individuals. It is an asset that belongs to the enterprise which needs to be managed. Assignment of data ownership within an organization becomes significant—whether it is for the purpose of accountability, defining retention and deletion policies, creating trusted data or eliminating redundancies. An organization needs to determine and assign an 'owner' within the organization who will make final decisions with respect to the data. It could be a single owner or multiple (i.e., different owners for financial, product and customer data). However, not assigning data ownership within the organization could lead to different departments taking different decisions with respect to the data and leading to a frustrating customer experience (let's not forget the customer's right to data portability and erasure).

3.40 COMPARITIVE LAW ANALYSIS OF DIFFERENT LEGISLATIONS

3.40.1 India

Due to the mechanical inefficiency of the provisions of Information Technology Act, 2000, the government authorities were compelled to ponder the rising concerns of privacy of individual data, which

is now considered a matter of national security. The Indian government‘s endeavor

to regulate the collection and use of personal data dates back to 2012 when the committee led by Justice A.P. Shah[101] released its report on privacy. To fully comprehend the privacy concerns and to come up with a viable Bill to address all these issues, the Government of India formulated a data protection committee under Justice B.N Srikrishna. The committee filed its report, commonly known as the Srikrishna Committee Report[102] on July 28, 2018. Thereafter, the draft Personal Data Protection Bill, 2018 was tabled in the parliament. Afterwards, a revised Personal Data Protection Bill, 2019 (hereinafter referred to as PDP Bill, 2019) was introduced by the
―Ministry of Electronics and Information Technology‖ in the ―seventeenth Lok Sabha‖ on December 11, 2019. The committee was constituted by the Ministry of Electronics & Information Technology, Government of India. The Bill was withdrawn in July 2022. The Bill was broadly based on the framework of the General Data Protection Regulation of the European Union and on the principles of the landmark judgement of the Hon'ble Supreme Court of India in justice K.S. Puttaswamy (Retd.) & Anr. V Union of India & Ors.[103] The Bill if implemented would have come in suppression of Section 43A of the Information Technology Act, 2000[104] (The IT Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the IT Rules) which was enacted under section ―43A of the IT Act‖[105].

The definition of ―Personal Data‖ has been enhanced in the Bill. The definition says that ―personal data‖ would be any data which directly or indirectly identifies a natural person. The Bill also directs any Data Fiduciary to store a copy of data (personal) on Data Centre located in India.

3.40.1.1 DIFFERENCES BETWEEN INDIA DATA PROTECTION BILL AND EU'S GENERAL DATA PROTECTION REGULATION

The GDPR in terms of data regulation is not just stringent but also a comprehensive law, so much so that it has become a common noun as a data protection regulation. The Indian drafters

[101]Justice AP Shah, Former Chief Justice and Delhi High Court, _Report of the Group of Experts on Privacy'.
[102]Srikrishna Experts Commitee, _A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' (2018) 2018 176 <https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf>. Accessed on 23 September 2019.
[103]_Justice K. S. Puttaswamy (Retd.) and Anr. vs Union of India And Ors.'(2017) 10 SCC 1.
[104]MA Yadugiri and Geetha Bhasker, _The Information Technology Act, 2000' (2011) English for Law 482. [105]"The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011(2011) 3".

appointed under Justice B N Srikrishna[106] for the purpose of preparing a draft legislation has repeatedly referred to GDPR in the draft of the Bill as well as the White Paper released by the committee. The Indian Bill is on the same lines as GDPR in terms of lawful processing, consent etc. There are few differences as well.

(1) Indian Bill does not require to share names and categories of personal data recipients by the ―Data Fiduciary‖ with the ―Data Principle‖.

(2) In the Indian Bill ―Data Fiduciary‖ has no obligation to share how long the data will be kept and stored with the ―Data Principle‖.

(3) ―Data Fiduciary‖ has no obligation to share the origin/source of data with the ―Data Principle‖.

(4) Under Indian Bill there is no obligation to share presence of automated decision making by the ―Data Fiduciary‖. Under European GDPR ―Data Subject‖ has to be provided with a copy of the data that is undergoing any sort of processing.

(5) ―Data Subject‖ under GDPR is required to be served with a copy of ―data that is being processed‖. Whereas on the other hand Indian Bill just asks for the summary of such data.

(6) When there has been a case of data breach, Indian Bill, does not require to share such information with ―Data Principle‖. The decision regarding this would be taken by ―Data Protection Authority‖.

3.41.1 Brazil

General Data Protection Law ("LGPD")

Brazil approved the LGPD on August 14, 2018[107]. The LGPD provided for an 18-month transition period and came into effect in 2020. Under this law data protection regime was established which defined rules for storing as well as processing ―personal data‖ both physical and electronic.

[106]Experts Commitee (n 102).
[107]de Souza and others (n 86).

Under the Brazil (LGPD) law, consent has to be obtained from the ―Data Subject‖ before processing any ―personal data‖, this provision is similar to the European GDPR. Under the said law consent has to be obtained in such a manner, whether in writing or any other means that it clearly indicates the will of the ―Data Subject‖. The subject over his data must have easily accessible information which should be made available in ―clear, adequate and ostensible manner.

Key Provisions in Comparison with the GDPR.

Provision	**LGPD**	**GDPR**
Definition of Sensitive Personal Data	Under this law Sensitive Personal Data is defines on similar lines as that of GDPR. Sensitive Personal Data includes data related to religious beliefs, health, sexual orientation which deeply identifies natural person.[108]	Under GDPR Sensitive Personal Data has been defined under Article 9 to include special category data revealing sensitive personal information of a man's life. It can be related to biometric, religious beliefs, sexual orientation etc.[109]
Whose Information is Protected?	Natural persons resident in Brazil.[110]	Natural persons resident in the European Union.
Case where Consent can be waived	When ―Data Subject‖ have already made their personal data public.	No similar exemption.
Processing Children's Data	While processing the data of children a separate and specific consent has to be	The GDPR clearly defines that for a child below 16 years consent from parent is

[108]Artur Potiguara Carvalho and others, _Big Data, Anonymisation and Governance to Personal Data Protection', *ACM International Conference Proceeding Series* (2020).
[109]Microsoft (n 1).
[110]de Souza and others (n 86).

	obtained by the parent or guardians. The law does not define the age wherein parental consent is required.[111]	an obligatory requirement.
Anonymized Data	Under Article 12, it is stated that any data even if it is anonymized will be considered as ―personal data‖ when it can be used to build behavior profiles of an individual.[112]	GDPR has no provision related to anonymized data. GDPR defines "pseudonymization", under this the data cannot be attributed to a specific person without adding any information to the existing data. The additional information if available is kept separately and the organization has to make sure that personal data is not merged with such additional information still pseudonymize personal data does not change the definition or status of personal data, and, thus, remains same and within the ambit of GDPR.[113]

[111]de Souza and others (n 86).
[112]ibid. [113]Microsoft (n 1).

3.41.3 Japan

In Japan the rights of individual in relation to their personal data came into effect in the year 2005. But as per the increase in the use of technology and focus of organizations shifting towards more and more use of ―big data‖ which was the root cause for the transfers of data cross border. All this change led to the requirement of amendment in law, therefore Protection of Personal Information[114] ("APPI") was amended and came into force on May 30, 2017.

―Personal Information‖ under APPI has been defined which shall include religion, race, personal information, medical history etc. This personal information has potential to bring about prejudice. The law applies to organization and businesses who are using information of people in Japan to offer goods and services, no matter if information of citizens is dealt with in Japan or outside, APPI shall apply. This act makes consent a necessary requirement for using Sensitive Personal Information. Taking consent is not enough under this law ―explicit purpose‖ should be mentioned by Data Handlers.

3.41.4 Singapore

Personal Data in Singapore is protected under Personal Data Protection Act, 2012[115] ("PUPA"). The act came into effect in different phases. First on 2nd January, 2013 Personal Data Protection Commission was formed. After that Do Not Call Registry[116] was implemented. Finally, on 2nd July, 2014 Data Protection Rules were implemented.

Under this law ―Personal Data‖ is defined as ―Data‖ about an individual whether true or false and the individual can be easily identified with the help of such data, the access of such data is held by the organization. The Data Protection law in Singapore has extraterritorial reach. Even though consent under Singapore

[114]Hideo Yasunaga, _Protection of Personal Information in Real-World Data in Japan‘ (2020) Annals of Clinical Epidemiology 177.
[115]Benjamin Wong Yongquan, _Data Privacy Law in Singapore: The Personal Data Protection Act 2012‘ [2017] International Data Privacy Law.
[116]―Warren B Chik, _The Singapore Personal Data Protection Act and an Assessment of Future Trends in Data Privacy Reform‘, *Computer Law and Security Review* (2013).‖

law is an explicit requirement, still there are quite a few exceptions as well. For example, data been used for ―artistic or literary purpose‖, data already available in public etc.

There is a provision under Singapore law which is totally in contrast with GDPR[117], the way how consent is dealt under PDPA, Section 15 is unique. This Section provides that if a person voluntarily gives data without giving actual consent to an organization, it is considered valid procedure under law. On the other hand, under GDPR it is mandatory that consent must be unambiguous, explicit, expressed and free. Thereafter an Amendment Bill was also passed in November 2020.

3.41.5 Hong Kong

Personal Data Privacy ("Ordinance")[118] governs data protection in Hong Kong. There are ―6 Data Protection Principles‖ mentioned in the ordinance which governs the privacy and data of individual. Under the said law ―Personal Data‖ is defined as data through which a person can be identified and also such data can be accessed in practicable form. The personal data under the Hong Kong law starts from name, address, medical records, identity card, employment record etc.

There are major differences when we compare EU GDPR with Hong Kong law. GDPR has wide applicability whereas the Ordinance of Hong Kong applies to personal data that is ―collected, processed and used‖ in or from Hong Kong.

Consent provisions are also very different in Hong Kong. Consent under the Ordinance is not a ―pre-requisite‖ for obtaining personal data. The Ordinance also doesn‘t have any provision related to parental consent nor does there is any

[117]―Graham Greenleaf, _Asia-Pacific Free Trade Deals Clash with GDPR and Convention 108‘ [2019] SSRN Electronic Journal.‖
[118]Rebecca Ong, _Data Protection in Malaysia and Hong Kong: One Step Forward, Two Steps Back?‘ (2012) Computer Law and Security Review 403.

requirement of breach notification to be given. The law under GDPR imposes heavy fine and penalty whereas under the Ordinance Section 50 Privacy Commission cannot impose fines or penalties first an Enforcement Notice to data handlers if they do not comply penalties are prescribed. There has been a discussion paper which proposes amendments to this Ordinance.

3.41.6 Canada

Canada has exhaustive law to protect right to privacy, also to see effective working and compliance of these laws there are several organization and agencies. In Canada there are two acts in relation to privacy, these acts are enforced by Privacy Commissioner-:

(a) ―Privacy Act‖- Information handled by federal government.

(b) Personal Information Protection and Electronic Documents Act[119] ("PIPEDA")- How businesses, organizations will use and handle personal information.

Key areas where the PIPEDA and the GDPR differ:

Provision	PIPEDA	GDPR
Consent	Consent is essential under PIPEDA. Under Section 6(1), the agreement of an individual to whom the organization's activities are directed is required on additional grounds, such as the individual's knowledge of the nature, purpose, and consequences of the	In contrast to the situation in Canada, where permission is the exclusive basis for collection, use, and disclosure (with limited exceptions), the GDPR allows for the acquisition of personal data on other bases, such as the fulfilment of a contract or legitimate interests. The GDPR lacks a notion of

[119]Derek Lackey and Neil Beaton, _The Current State of Data Protection and Privacy Compliance in Canada and the USA‘ (2019) Applied Marketing Analytics 84.

	collection, use, or disclosure of their personal information. PIPEDA has no stated consent requirement. However, Consent is in accordance with Sensitivity of the data and how the individual expects how his/her information will be handled, Schedule 1, cl. 4.3.5).[120]	implied consent as well.
Consent of Children	Privacy Commissioner suggested that Children below age of 13 will not be able to give consent which is meaningful consent in such cases consent must be taken from parents and guardians.[121]	The GDPR has set the minimum age of consent oat 16 years of age.
Data Breach Reporting	As of November 1, 2018, organisations subject to (PIPEDA) are required to report to the Privacy Commissioner of Canada breaches of security safeguards involving	All breaches are to be notified within 72 years.

[120]Lisa M Austin, _Is Consent the Foundation of Fair Information Practices? Canada's Experience Under PIPEDA' (2006) University of Toronto Law Journal 203.
[121]The Office of Privacy Commissioner of Canada, _Summary of Privacy Laws in Canada' (*Summary of privacy laws in Canada*, 2018).

	personal information that pose a real risk of serious harm to individuals, notify affected individuals about these breaches, and maintain records of all breaches. There is no prescribed time and the notification to individuals is to be sent as soon as	
Data Protection Authority	Under PIPEDA, the federal Privacy Commissioner may make non-binding recommendations to organizations but cannot issue binding orders or levy administrative fines.	The supervisory authority possesses investigative powers (e.g., to conduct data protection audits), corrective powers (e.g., to issue warnings and reprimands, to order an organisation to bring processing operations into compliance with the GRPR, and to order an organisation to notify affected data subjects of a data breach), and advisory powers (e.g., to accredit certification bodies, to adopt standard data protection clauses, and to approve binding corporate rules).
Fines	The Federal Court may impose fines of up to $100,000 if: I an employer fires, suspends, demotes,	Depending on the circum-stances, administrative fines of up to: €20 million;

	punishes, harasses, or otherwise discriminates against a whistleblower employee; or (ii) an employer retaliates against a whistleblower employee. (iii) where a person obstructs the federal Privacy Commissioner during an inquiry or audit.	4% of annual worldwide turnover (whichever is higher)

3.41.7 United States

US Health Insurance Portability and Accountability Act (HIPAA)

Both the GDPR and HIPAA[122] share several commonalities. These are extremely comprehensive sets of regulations and are committed to the goal of protecting privacy. Both regulate how protected information/data is collected, used, disclosed, maintained, transmitted, disposed of, kept secure, etc. Under both the regimes, individuals/data subjects can exercise comprehensive rights about their data/information.

	GDPR	**HIPAA**
Consent	Permits the use of health-related personal data with the subject's express permission, unless EU or	PHI use or disclosure can only be made after receiving an authorization from the individual such authorization

[122]Wilnellys Moore and Sarah Frye, _Review of HIPAA, Part 1: History, Protected Health Information, and Privacy and Security Rules‘ (2019) Journal of Nuclear Medicine Technology 103.

	member state legislation prohibits the use of consent. Under ―Explicit consent‖ the consent taken for processing must be of higher value and standard when compared to the consent obtained for processing other forms of A person must be explicitly informed of how their data will be used and must take deliberate action to indicate their permission.	includes number of elements.[123]
Employment, social security, and social protection responsibilities	Allows the Sensitive Personal Information to be processed when there arises an obligation under any collective agreement in relation to employment, social security etc[124].	The law allows to the extend permissible by law. Usually processing of such data is prohibited for employment purposes[125].
Protecting vital interests when the subject is	Protecting the interests of Data Subjects who are physically or legally incapable of providing	Permission has to be obtained from the representative of an individual who is incapable of giving of giving consent by

[123]Ozgur Kafali and others, _How Good Is a Security Policy against Real Breaches? A HIPAA Case Study‘, *Proceedings - 2017 IEEE/ACM 39th International Conference on Software Engineering, ICSE 2017* (2017).
[124]Electronic Frontier Foundation, _Genetic Information Privacy‘ (2020) GINA, HIPAA and Genetic Information Privacy 55.
[125]Michele E Gilman, _Five Privacy Principles (from the GDPR) the United States Should Adopt To Advance Economic Justice.‘ (2020) Arizona State Law Journal 74.

incapable of providing consent	permission may necessitate the processing of sensitive personal information.[126]	himself/herself.
Not-for-profit entities	Entities that are not-for-profit are entitled to process data even if they use it for political, intellectual, religious, or trade union purposes. The processing of member or former member data must be controlled, and such data may not be transmitted to a third party without prior authorization.	No such provision.
Information already made —public‖ by the subject	Data that has been made accessible to the public by the Data Subject may be handled by the entities.	Differs from the GDPR in that such use or disclosure by the Data Subject has no bearing on the HIPAA safeguards.[127]

3.41.8 California

California (CA), on June 28, 2018, passed a data privacy law that grants consumers greater control over their personal information. This law was subsequently amended in September 2018. The AB 375 or the California Consumer Privacy Act of 2018 ("California Act" or the "CCPA") which goes

[126]S Alder, A Kelleher and S Greene, _HIPAA Compliance Guide‘ (2017) HIPAA Journal 118.
[127]Merrick and Ryan (n 53).

into effect on 1 January 2020, is being hailed by many as one of the strictest online privacy laws in the United States. Upon the implementation of the California Act, businesses will be required to comply with extra restrictions regarding the processing of the personal information of California residents. Before a business can collect any personal information, the California Act requires the business to inform the consumer of the categories of information it will collect and the purpose for which it will be used (including any sale). Businesses are also required to provide an online privacy policy that provides:

(1) a description of the consumers' right to know, right to equal service and price; (2) methods for submitting requests pursuant to their right to know; and

(3) a list of the categories of personal information it has collected, sold or disclosed in the past 12 months or the fact that it has not sold or disclosed any personal information. Businesses that sell personal information must have a prominent link on their site labelled Do Not Sell My Personal Information and enable customers to opt out of having their information sold to third parties. Few important points to note here:

(i) The law comes into effect from January 1, 2020.

(ii) It offers citizens of California the right to ban the sharing of personal information, the right to seek access and deletion, and the right to statutory damages for security breaches without demonstrating injury.

(iii) The Act allows the Attorney General of California to adopt regulations after collecting public opinion.

(iv) It mandates the delivery of personal information gathered, sold, exchanged, or otherwise revealed during the previous twelve (12) months.

(v) It is expected to be changed by legislation submitted during the 2019-2020 legislative session.

Applicability

The California Act applies to all 'businesses' that serve California residents and has a wide definition of the term "Business" which means[128]:

(i) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organised or operated for the profit or financial benefit of its shareholders or other owners, that collects the personal information of consumers, or on whose behalf such information is collected, and that alone, or jointly with others, determines the purposes and means of processing consumers' personal information, and that conducts business in the United States.

(ii) Has annual gross revenues in excess of $25,000,000; Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices; Receives 50 percent or more of its annual revenues from the sale of consumers' personal information.

(iii) The word "Business" also encompasses an entity that manages or is controlled by a business (as described above) and that has similar branding with the business (defined as a shared name, service mark, or trademark).

Some important points to note about the applicability of the CCPA are[129]:

(a) The law does not require that one should have physical operations in California.

(b) It applies to any entity that controls or is controlled by a "business" as defined above.

(c) It applies to parent companies and subsidiaries sharing "common branding".

[128]Lothar Determann, _New California Law Against Data Sharing‘ [2018] Computer Law Review International.
[129]Nicholas F Palmieri, _Who Should Regulate Data? An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws‘ (2020) Hastings Science and Technology Law Journal 554.

(d) It exempts I non-profit organisations that do not operate for profit or financial gain; (ii) healthcare providers governed by California's Confidentiality of Medical Information Act (CMIA) or covered entities governed by the Health Insurance Portability and Accountability Act (HIPAA); (iii) consumer reporting agencies to the extent that their use of personal information is limited by the federal Fair Credit Reporting Act (FCRA).

Comparison with the GDPR

In certain ways, the CCPA and the GDPR are comparable, but they're not the same. Both terms have wide meanings when it comes to personal data/information. Both of these pieces of law add formal compliance requirements to the protection of personal data and information. Both may result in significant regulatory fines and penalties.

There are, however, a lot of distinctions. Here's a rundown of the distinctions[130]:

(i) Unlike the GDPR, California's data protection regulations are neither repealed or replaced by the CCPA.
(ii) The CCPA provides safeguards depending on where a person lives.
(iii) Processing of personal information is not prohibited by default under the CCPA.
(iv) Data minimization is not required under the CCPA.
(v) Businesses are not obligated to maintain records under the CCPA.
(vi) Appointment of a Data Privacy/Protection Officer or an equivalent is not required under the CCPA.
(vii) No right to correction exists under the CCPA.
(viii) International transfers are not subject to any particular limitations under the CCPA.

The table below sets, out a comparison between the key provisions of the California Act with the GDPR;

[130]Sahara Williams, _CCPA Tipping the Scales: Balancing Individual Privacy with Corporate Innovation for a Comprehensive Federal Data Protection Law‘ [2021] Indiana Law Review 114.

Provision	California Act	GDPR
Definition of Personal Information	The word "personal information" is defined more broadly under the California Act. Personal information is defined as data that identifies, relates to, characterizes, is capable of being connected with, or might reasonably be linked, directly or indirectly, with a specific consumer or household.	—Any information pertaining to an identified or identifiable natural person‖ is included in the GDPR's wide definition. The California Act, on the other hand, includes categories like as education information and business information that are not covered by the GDPR.
Where is Information protected?	The CCPA protects "consumers," who are defined as natural people "resident" in the state of California. Note: While the CCPA claims to include workers who live in California, AB 25 would change the definition of "consumer" to exclude employees, contractors, agents, and job seekers.	Natural persons resident in the EU.
Opting out vs Opting In	Consumers must "opt out of having their data sold", and businesses must offer a user-friendly method for	For processing to take place, the data subject's explicit permission is needed.

	submitting opt-out requests.	
Requirement for Data Processing	Unlike the GDPR, the California Act states that data cannot be processed when a consumer has opted out, but it does not specify particular circumstances in which data may be handled.	When there is a particular legal basis, such as consent, contract fulfillment, protecting a person's vital interests, public interest, or the controller's or a third party's legitimate interest.
Right of Data Subjects	• Right to be informed of the types of information collected and the purposes for collection. • Right to access[131] the categories, sources, and specific pieces of information collected, the purposes for data collection, and third parties with whom the data has been shared. • Right to request deletion of personal information[132]. • Right to opt out of the sale of a consumer‘s	• Right to be informed of data processing practices. • Right to access personal data and other information about processing. • Right to rectification. • Right to be forgotten. • Right to restrict processing. • Right to data portability. • Right to object to processing. • Right not to be subject to a decision based solely on automated processing.

[131]ibid. [132]ibid.

	personal information[133]. • Right to receive services[134] on equal terms. Contrary to what the GDPR sets forth, ―the CCPA does not mandate data minimization, nor does it impose the right to rectify / correct personal information‖.	
Processing of Information of a Child	A business cannot knowingly sell data of a customer under the age of 16 unless[135]: • the consumer is between the ages of 13 and 16; or • the parent or guardian of the child is under the age of 13 has opted in to the sale.	It is legal to process children's data if the kid is at least 16 years old; else, parental permission is needed. The GDPR also allows member states to reduce the age of parental permission to no less than 13 years old.
Fine	Between $100 to 750 per consumer each occurrence for private causes of action, or actual damages, whichever is higher. Civil fines of up to $7,500	Administrative penalty of up to €20 million or 4% of the preceding year's worldwide annual revenue, depending on the violation.

[133]ibid. [134]ibid.
[135]Kimberly Dempsey Booher and Martin Robins, _American Privacy Law at the Dawn of a New Decade (and the CCPA and COVID-19): Overview and Practitioner Critique‘ (2020) SSRN Electronic Journal 44.

	per violation for CAG acts. Specifications: Businesses may suffer civil fines of up to $7,500 per purposeful violation and $2,500 per accidental violation in actions conducted by the California Attorney General; corporations would have thirty (30) days to fix any alleged violation after receiving notice of the alleged violation. In private proceedings, consumers may seek statutory damages of not less than $100 and not more than $750 per consumer per occurrence, or actual damages (regardless of whether actual losses have been shown), whichever is larger. In private proceedings, consumers may seek declaratory or injunctive relief, as well as any other	

	remedy the court deems appropriate. In any case initiated by the California Attorney General, companies might be subject to an injunction.	
Transfer of Data Between Countries	The California Act does not contain any relevant restrictions in this regard.	Adequacy measures are necessary for any nation found to have legislation that differ from those of the EEA.
Data Processors	If the business wishes to exclude the transfer of personal information to the business from the definition of the sale of personal information, it must enter into a written agreement with the third party. If the service provider exemption is satisfied, the company may continue to share information with them even if the California resident expresses a desire for their personal information not to be sold.	Controllers must enter into a written contract with processors that handle a data subject's personal data that meets specific conditions.
Data Breach Notification	The California Act, unlike the GDPR, does not	A privacy breach must be reported to the data subject

	require a company to notify a customer of a data breach.	within 72 hours by the Controller[136].
Higher Charges for Opt Out	Consumers who opt out of having their data sold can pay a greater fee as a result of the California Act.	No equivalent provision in the GDPR.
Incentives for Data Sale	Businesses have the right to provide non-monetary incentives in return for reselling a customer's personal data.	No equivalent provision in the GDPR.

Personal information is defined more broadly under the CCPA than it is under California's breach reporting legislation (described below). It's worth noting that the CCPA's definition of personal information is broader than the GDPR's in that it includes "household" (despite the fact that the CCPA doesn't define "households"). Personal information as defined by the CCPA excludes the following information[137]:

(i) Publicly available information (data from federal, state, or municipal government records that is lawfully made available).
(ii) customer data that has been "de-identified" or aggregated.
(iii) information gathered, utilized, sold, or disclosed under the GLBA or the Driver's Privacy Protection Act (1995), but only to the extent that the CCPA "conflicts" with those statutes.

[136]Elif KiesowCortez, _Data Breaches and GDPR‘, *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (2020).
[137]Jeeyun (Sophia) Baik, _Data Privacy against Innovation or against Discrimination?: The Case of the California Consumer Privacy Act (CCPA)‘ (2020) Telematics and Informatics 67.

(iv) When personal information is "reported in, or used to generate," a consumer credit report, it is sold to or from a consumer reporting agency (as defined in the Fair Credit Reporting Act or the FCRA).

Here's a quick rundown of the most important CCPA regulations for businesses:

- Inform the public about the collection practices.
- Make a statement of customers' rights available and keep it up to date at least once every twelve (12) months.
- Separately list all categories of personal information that was collected, sold, or revealed for a business purpose in the last twelve (12) months.
- Give advance notice of all onward transfers.
- Make two or more designated means for submitting requests for information available to consumers to help them with their requests.
- Implement and maintain adequate security measures, methods, and practices to ward off the private right of action created by California Civil Code Section 1798.150.
- If you're selling personal information, give people the option to opt out via a prominent link that says, Don't Sell My Personal Information.
- If selling, get consent from customers aged 13 to 16, as well as parents if the consumer is under 13.

To achieve CCPA compliance, businesses must establish privacy teams and key points of contact, as well as secure an adequate funding for CCPA compliance initiatives.

- Conduct assessments to establish the components of a CCPA compliance program that is appropriate.

- To comply with the CCPA's standards, create and update privacy policies, practices, and notices.

- Raise awareness of the CCPA and provide CCPA training.

- Create and update privacy notices and consent protocols, taking into account the unique requirements for kids' personal information.
- Create and improve ways to address the privacy rights of consumers.
- Make data breach and incident response protocols and keep them up to date.
- A data mapping exercise should be carried out.
- Create and update procedures for third-party management and sourcing.
- Ensure that suitable and acceptable security controls are implemented and maintained.
- Set up proper monitoring and testing procedures to ensure CCPA compliance.

As part of a deal with the sponsor of a similar privacy ballot measure that had qualified to be brought before state voters on Election Day in November 2018, the California Act was approved in an extremely expedited timetable. The sponsor had agreed to withdraw his ballot initiative if the California Act was signed into law before the June 28 withdrawal deadline. Given the speed at which the legislation was passed, it is certain that amendments to the legislation will be necessary in the next year and a half and it will be interesting to see the final shape that the legislation takes.

3.41.8.1 Incident & Breach Management — California Data Breach Notification Law

An entire part should be dedicated to the data privacy/security event and breach management system. First, let's look at California's Data Breach Notification Law.

(iv) If you do business in California.

(v) Own or licence electronic data.

(vi) The data contains personal information of California residents (hereafter referred to as CA Residents); There was unauthorised access to electronic personal information of CA Residents; and, The personal information is not encrypted; you are required to provide a data breach notification under this law

Personal information is defined by California law as an individual's first name or first initial and last name combined with any one or more of the following:

- your social security number;
- the number on your driver's license or identification card;
- account or card numbers, whether they're used in conjunction with a security or access code;
- health-related information
- information on health insurance; or
- Information gathered through a computerized license plate recognition system.

A username or email address, as well as a password or security question and answer, are examples of personal information that would allow access to an online account. Who needs to be informed? Any CA resident whose personal information has been compromised as a result of a data breach must be notified. Any company that is compelled to notify more than 500 California residents as a result of a single data breach must additionally send a single copy of the breach notice to the Attorney General of the state. If there has been actual or suspected unauthorized access to personal information, businesses that maintain (but do not own or license) the information must notify the entity that owns or licenses the information of any security breach.

The following information should be included in the aforementioned notification:

- the person sending the notice's name and contact details;
- a list of the different forms of personal data exposed in a data breach;
- the important dates related to the breach (a timeline);
- whether the delay in giving the notice/notification is due to a law enforcement agency's inquiry;
- abroad or high-level description of the breach;
- contact information for ―major credit reporting agencies‖ (CRAs) in the event that a social security number, driver's license number, or CA ID card number was revealed in the hack; and
- an offer to provide relevant security measures, such as identity theft prevention and mitigation services, if the organization notifying you is also the source of the incident.

A corporation can also give information about what has already been done to safeguard victims of the breach, as well as any advice on how victims can protect themselves, at its discretion.

It's how all of the above information is presented those matters. The following rules must be adhered to:

- It must be written in basic and straightforward language.
- The title must be Notice of Data Breach. It should be divided into the following sections:

- What went wrong?
- What information was compromised as a result of the breach?
- What exactly are you up to? What can the victim do?
- More information is available.

- All titles and headings must be shown "clearly and conspicuously."
- The font size must not be less than ten points.

The importance of the notification's timing cannot be overstated. Any corporation that possesses or leases computerised data containing personal information about California residents must tell impacted individuals as soon as is practicable and without undue delay. A business or organisation that stores digital data that belongs to or is licenced by another business or organisation must tell the owner of the breach "immediately upon discovery."

All notifications must take into account the justified need to collaborate or cooperate with law enforcement, as well as the procedures necessary to analyse the scope of the breach and restore the reasonable integrity of the data system. If a law enforcement agency believes that providing such notice may compromise an ongoing criminal investigation, the notice may be postponed. It should be noted that if a notification is to be delivered to more than 500 California residents, a copy of the notification must also be shared with the California Attorney General; however, no timetable is given.

The notification(s) must be sent in writing or electronically, as long as they comply with the provisions of the federal E-Sign Act, 15 U.S.C. 7001 et seq. If the cost of delivering notification exceeds $250,000, the number of people to be notified exceeds 500,000, or the business/company lacks appropriate contact information, notification can also be issued via a substitute notice.

The following information must be included in this substitution notice:

- An email notice (if the business/company possesses email addresses for the data subjects who are impacted);
- A prominent posting of the notice on the company's website (assuming the company has one) for at least thirty (30) days; and
- All major state-wide media are notified.

3.41 The Privacy Shield

The US Department of Commerce, the European Commission, and the Swiss Administration, respectively, designed the EU-US and Swiss-US Privacy Shield Frameworks[138]to in support of transatlantic commerce, offer a system for enterprises on both sides of the Atlantic to comply with data protection regulations when moving personal data from the European Union and Switzerland to the United States. The European Commission declared the EU- US Privacy Shield Framework acceptable to allow data transfers under EU law on July 12, 2016[139]. The Swiss Government declared on January 12, 2017 that the Swiss-US Privacy Shield Framework had been approved as a competent legal method for complying with Swiss standards for transferring personal data from Switzerland to the US.

(i) Self-Certification I

The Privacy Shield programme, which is administered by the International Trade Administration (ITA) of the U.S. Department of Commerce, allows U.S.-based companies to join one or both of the Privacy Shield Frameworks in order to benefit from the adequacy findings.[140]. To join any "Privacy Shield Framework," a U.S.-based organisation must self-certify to the Department of Commerce and publicly pledge to comply with the Framework's rules.[141]. Joining a privacy shield is a voluntary commitment, but once made, it is enforceable under US law.

During the self-certification process, an organization must submit information such as a description of its personal data privacy policy, the statutory body with jurisdiction to investigate claims against the organization for possible unfair or deceptive practices and violations of privacy laws or regulations, annual revenue, and contact information.

[138]Xavier Tracol, _EU–U.S. Privacy Shield: The Saga Continues‘ (2016) Computer Law and Security Review. [139]Privacy Shield Framework, _Privacy Shield | Privacy Shield‘, *Privacy Shield Framework (USA, Europe)* (2018). [140]Doron S Goldstein and others, _Understanding the EU-US ―Privacy Shield‖ Data Transfer Framework‘ (2016) Journal of Internet law 198.
[141]ibid.

(ii) The Privacy Shield

Framework through the EU US Privacy Shield Framework and the Swiss UID Privacy Shield Framework, the US Department of Commerce, according to its legislative power, established the Privacy Shield Principles and Supplemental Principles (collectively, "Principles"). Among these are[142]:

Notice: Before an organisation uses or processes such information for a purpose other than that for which it was originally collected or processed by the transferring organisation, or discloses it for the fiduciary purpose, a notice must be provided in clear and conspicuous language.

The notification must include[143]:

- information about the organization's involvement in the Privacy Shield; the organization's participation in the Privacy Shield.
- the organization's participation in the Privacy Shield; the organization's participation in the Privacy Shield; and the organization
- a list of the several forms of personal information gathered.
- a description of the reason for the data collection.
- a person's right to access his or her personal information.
- Whether it is[144]: (1) the panel established by DPAs, (2) an alternative dispute resolution provider based in the EU, or (3) an alternative dispute resolution provider based in the United States, the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual.
- submitting to the FTC's, the Department of Transportation's, or any other authorized statutory authority in the United States' investigative and enforcement powers.

[142]Martin A Weiss and Kristin Archick, _U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield‘, *The European Union: Challenges and Prospects* (2016).
[143]Article 29 Data Protection Working Party, _Opinion 01/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision‘.
[144]Sam Curry, _Achieving GDPR Compliance Post-Privacy Shield‘ (2021) Computer Fraud and Security 403.

- a person's right to invoke binding arbitration under specific circumstances.
- an obligation to disclose personal data in response to authorized requests from public authorities, such as to meet national security or law enforcement requirements; and
- its responsibilities in the event of third-party transfers.

Choice: The Principles require an organization to give individuals the option of opting out of having their personal information disclosed to a third party or[145] used for a purpose that is materially different from the purpose(s) for which it was collected or subsequently authorized by the individuals. Individuals must be given clear, visible, and easy-to-access tools to exercise their freedom of choice.

For sensitive information, organisations must get explicit express agreement (opt in) from people (i.e., personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or information specifying the sex life of the individual).

Accountability for Onward Transfer[146]: The Principles require organisations to enter into a contract with the third-party controller stating that the data may only be processed for limited and specified purposes consistent with the individual's consent, that the recipient will provide the same level of protection as the principles, and that the recipient will notify the organisation if it makes a mistake.

Security[147]: Taking into account the risks inherent in the processing and the nature of the personal data‖, the organization is obligated to take reasonable and

[145]U.S. DEPARTMENT OF COMMERCE, _Privacy Shield', *Privacy Shield Framework (USA, Europe)* (2016). [146]Dewi Sinta Hermiyanty, Wandira Ayu Bertin, _Guide to the EU-U.S. Privacy Shield' (2019) Journal of Chemical Information and Modeling.
[147]Laura Drechsler, _What Is Equivalent? A Probe into GDPR Adequacy Based on Eu Fundamental Rights' (2019]) Jusletter IT.

suitable measures to safeguard it against —loss, misuse, and unauthorized access, disclosure, alteration, and destruction.

Data Integrity and Purpose Limitation: Personal data must be limited to the purpose for which it was obtained, and the organization must take reasonable means to ensure that personal data is accurate, full, and current for its intended use.

Individuals must have access to their information and be able to edit, update, or delete it if it is inaccurate or has been processed in a way that violates the principles (with limited exceptions).

Recourse, Enforcement, and Liability: Organizations must have independent recourse processes in place to respond to individual complaints and requests for information from the Department about the Privacy Shield.

On Uncertain Footing: The Privacy Shield? On June 26, 2018, the European Parliament voted on a motion that questioned the efficacy of the EU-US Privacy Shield. According to the resolution, the current Privacy Shield arrangement does not provide the adequate level of protection required by Union data protection law and the EU Charter, as interpreted by the European Court of Justice, and unless the United States is fully compliant by 1 September 2018, the European Parliament requests that the Commission suspend the Privacy Shield until the US authorities comply. In response to the resolution, Vera Jourova, the EU Commissioner for Justice, wrote a letter to US Commerce Secretary Wilbur Ross on July 26, 2018, stating that the US has three months to comply with EU demands regarding the sharing of private data pertaining to EU citizens, and demanding that the US appoint an ombudsman to deal with privacy-related complaints from EU citizens. As of yet, there has been no announcement on the Privacy Shield's suspension. To add to the commotion, a coalition of technology and industry organizations sent a letter to US Secretary of State Rex Tillerson on August 20, 2018, urging him to appoint a Privacy Shield ombudsperson. The

fate of the Privacy Shield will be intriguing to watch, as will whether the EP decision leads to changes in US domestic data privacy laws.

The GDPR has more stringent regulations than the Privacy Shield. On Friday, anything you do remotely in Europe will be subject to GDPR in its entirety, and Privacy Shield will no longer be considered a "free pass" for US companies to use the data as they want, according to Giovanni Buttarelli, the EU's Data Protection Chief, to the EU Observer. Organizations in other Non-EU nations that deal with data of EU residents must comply with the GDPR, and Non-EU countries must overhaul their existing legislation to ensure that their data protection laws are deemed "sufficient" by the European Commission.

3.42 Conclusion

The GDPR is now the most stringent data protection regime in the world with most other countries regarding it as the "gold standard". As seen in the table above, the number of data protection laws is expanding globally, with many being modelled after the EU Directive, the GDPR, or the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. According to UNCTAD's data protection tracker, 107 nations (of which 66 were emerging or transition economies) have enacted data protection and privacy laws. Less than forty percent of nations in Asia and Africa have enacted legislation in this area. The data may be summed up as follows:

58 percent of nations having legal provisions 10 percent of nations have legislative

draughts 21 percent of nations without any laws

12 percent of nations without data

I. African continent (54 countries) 23 Legislation (43 percent)

Draft Legislation: 7 (13 percent)

Absence of Legislation: 12 (22 percent)

No Data: 12 (22 percent)

(2) America (35 countries)

Constitution: 18 (51 percent)

Draft Legislation: 8 (23%)

No Legislation: 9 (26%)

No Data (0%)

III. Asia-Pacific (60 countries) Legislation: 27 (45%)

Draft Legislation: 4 (7%)

No Legislation: 19 (32%)

No Data: 10 (17%)

IV. Europe (45 countries) Legislation: 44 (98%)

Draft Legislation: 0 (0%)

No Legislation: 0 (0%)

No Data: 1 (2%)

V. Least Developed Countries (47 countries) Legislation: 17 (36%)

Draft Legislation: 3 (6%)

No Legislation: 17 (36%)

No Data: 10 (21%)

VI. Small Island Developing States (29 countries) Legislation: 9 (31%)

Draft Legislation: 4 (14%)

No Legislation: 10 (34%)

No Data: 6 (21%)

Capacity of policy makers, available resources for monitoring, existing/current enforcement systems, and the existing political climate around national security —all of these have made the GDPR and OECD inspired frameworks difficult around the world. Specifically, when it comes to trade negotiations, there is increasing pressure to tone down stringency, as stringent data protection is perceived to be a barrier to trade. Additionally, there are concerns that "copy- pasting" data protection clauses from other countries will most likely not work as there are different enforcement parameters, or market surveillance infrastructure, and there are different cultural norms that are at play in different jurisdictions. We can only wait and watch for further developments in this space.