

**ICT 2**

**Implementation and Commissioning**

(CP5047)

**Research Report**

**On**

**Privacy Policy**

**Aditya Walunj**

**26th May 2019**

**Table of Content**

Abstract……………………………………………………………………………….………3

Introduction…………………………………………………………………………….……..4

Privacy Laws…………………………………………………………………………….……5

1. Privacy Act 1988 (Australia)………………………………………………….…..5
2. Data Privacy Law in India…………………………………………………….…..5
3. Privacy Law for websites and apps in the United States……………………….…6
4. GDPR Compliance………………………………………………………………..7
5. User Rights under GDPR…………………………………………………………8
6. Data Privacy Laws pertaining to their region……………………………………..9

Privacy Policy in Brett’s Planner…………………………………………………………….10

Brett’s Planner Privacy Policy (as displayed on website)……………………………………11

Conclusion……………………………………………………………………………………14

References……………………………………………………………………………………15

**Abstract**

Over the past few years, cyber security attacks and internet spams have seemingly increased causing heaps of private data to be leaked over the internet. Data protection is one of the top priorities for organisations as well as it’s users. Inclusion of privacy policy in websites and applications have become mandatory by law and an essential document in building the trust between organisation and its customers or users. This research report presents the Privacy protection laws of different countries and why including a privacy policy is required for businesses and organisations.

**Introduction**

A privacy policy is a legal document or a set of statements that explains how an organisation, or a company handles any customer, client or employee information gathered in its operations. It’s an extremely essential and necessary document required for a website or mobile application. A privacy policy page specifies how any personal identifiable information is gathered such as names, address, date of birth, ID numbers, email id, contact number, credit card information as well as other things like location, browser’s IP address, browsing habits, order history, uploads and downloads, etc. It also discloses on how it intends to use, share, sold or transfer the user’s data collected by the organisation’s website and for what purpose. (Rouse, 2013) Privacy policies are commonly displayed on organisation’s website for users to understand how the information they share will be dealt legally by the organisation. This policy is made viewable to customers or users interacting or visiting a website, but it can also be printed on paper. Privacy laws differ for different countries and continents but they’re almost similar in operation. (Unknown, 2019)

Privacy Policy is required by the law if organisations are collecting personal information of website users. It must be displayed by the websites or applications to the users to review the privacy practices of the organisation. People are concerned about their private information being handled by organisations, most of us would like to feel secure while typing in our private information like home address and telephone number. Privacy Policy is a great means of communication for the visitors of the website to trust the website organisation. (Pegarella, 2017)

**Privacy Act 1988 (Australia)**

The federal Privacy Act 1988 was designed in March 2014 to promote the protection of individual’s privacy in Australia by imposing obligations on those who collect and handle personal information to manage it responsibly and transparently. Privacy Act 1988 includes number of principles known as Australian Privacy Principles (APPs). These principles are similar to other jurisdictions such as Europe’s GDPR and Canada’s Privacy Act. Initially the Privacy Act applied to Commonwealth government agencies and departments, but now it also applies to the private sector. The Privacy Act 1988 applies to a medium to large business organisations and companies that collect, handle, share or store personal information of individuals. Not just organisations but even individuals, partnerships, unincorporated associations and trusts may require a Privacy Policy. The Office of the Australian Information Commissioner (OAIC) monitors APPs compliance in Australia. (OAIC, 2019)

**Data Privacy law in India**

Data Privacy regulations regarding privacy policies in India can be found mainly in Information Technology Act, 2000, Information Technology Rules, 2011 and India’s ministry of Communications. At the moment, India does not have its own Data Protection Law but it’s going to have one soon after a Committee headed by a retired Supreme Court judge BN Srikrishna submitted an initial assessment and recommendations on data privacy and management as well as a draft of the legislation on data protection titled Personal Data Protection Bill, 2018. For a long time, major Indian companies and organisational bodies are vying for an Indian Privacy Law that will safeguard user information and help accelerate India’s fast-growing digital economy. The draft bill includes jurisdiction of processing private data, setting up an independent regulatory body for enforcing the data protection law and heavy penalties for violations among other causes. India’s online market is second to China and the internet penetration has been on a rapid incline since the last decade thanks to the growth of start-ups, e-commerce companies and technology offerings across industries. Until now, the accepted legal framework for the Indian Privacy Policy is offered by the Information Technology Act, 2000 which provides norms for collection of data and its usage. The Information Technology Act 2000 however does not go deep into elaborating guidelines for data storage techniques, user consent as well as norms for data processing. The draft of Data Protection Law is expected to cover this. (Balaji, 2018)

**Privacy Law for websites and apps in the United States**

Although there is no single omnibus law in the US governing American companies and organisations to require a privacy policy, there are various federal and state laws that require them to be implemented by all the organisations in all the American states. The Federal Trade Commission (FTC) takes charge of regulating data protection of all the website users in the USA.

American State and Federal laws that provide data privacy framework –

1. The Consumer Credit Reporting Control Act
2. The Computer Security Act 1997
3. The Computer Fraud and Abuse Act of 1986
4. The Americans with Disability Act
5. The Cable Communications Policy Act of 1984
6. The Americans with Disability Act

California is home to major tech giants like Google, Facebook and Apple and therefore they have their own Data Protection law to comply with Californian laws. Organisations or businesses collecting personal information of Californian residents are required to implement a Privacy Policy on their websites and applications. The California Online Protection Act of 2003 (CalOPPA) is also the first state law which requires American organisations or business collecting personal identifiable information of Californian residents to host a Privacy Policy. (TermsFeed, 2016)

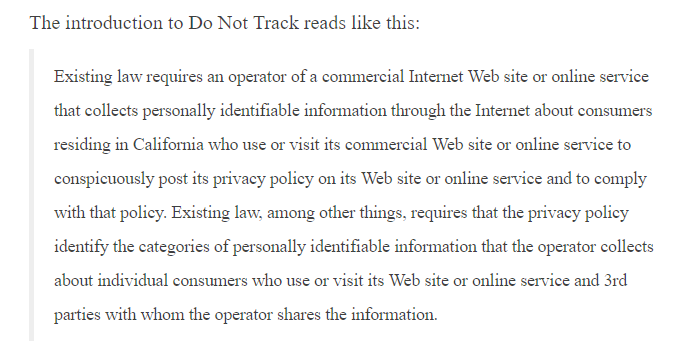


Figure 2: A statement from the CalOPPA guidelines.

**GDPR Compliance –**

GDPR (General Data Protection Regulation) handles data and information privacy in the European Union. It specifies how private data should be lawfully collected, used, protected and processed by organisations within EU and beyond who interact with EU organisations or individuals. PR is considered to be the most important change in data privacy regulation in the last two decades, it’s the core of Europe’s digital privacy legislation. GDPR was approved by the EU Parliament on 14th of April 2016 and was put into effect since May 25th, 2018 replacing the previous Data Protection Directive Act. The regulation is designed to harmonize data privacy laws in Europe while emphasizing on protecting and empowering European Union citizens data privacy. It intended to strengthen data protection for all citizens who share their personal information on websites, apps, etc to fall within the scope of application putting private and personal information control back into their hands. GDPR defines personal data as any information relating to identified or identifiable natural person including names, date of birth, email address, pictures, IDs, location, online identifiers and one or more factors specific to their physical physiological, genetic, mental, economic, cultural or social identity. GDPR aims to give EU citizens added control on their personal information with it’s new set of rules and simplify regulatory environment for business so both citizens and businesses in the European Union can fully benefit from the digital economy. Organisations handling data on a large scale have a Data Protection Officer (DPO) responsible for overseeing organisation’s data protection strategy and its implementation to ensure compliance with GDPR requirements. The new regulation framework applies to organisations in all member-states and has implications for business as well as individuals in Europe. It also applies to organisations outside the European Union which interact for businesses, services or goods with EU or its citizens. This calls for almost every major corporation in the world to comply with GDPR. Organisations that fail to comply with GDPR provisions can be fined as much as 20 million euros or up to 4 percent of their annual global turnover (whichever is greater). GDPR promotes greater transparency and accountability and aims to increase public trust by giving individuals getting more control over their personal data. By getting data protection right organisations enhance their reputations and build better trusted relationships with existing and potential customers. Implementing and maintaining the technical and organisational measures required by the GDPR, organisations benefit from greater levels of information governance and cyber resilience which will help them mitigate the daily onslaught of cyber-attacks. (Palmer, 2019)



**User Rights under GDPR –**

1. **Right to be informed**: Users or an individual have a right to be informed by the organisation that they’re collecting their data for particular purposes. In addition to this, users also need to be informed why the organisation is collecting their data, how long they intent to keep that information and whom would they be sharing with.
2. **Right of access**: Users or an individual are entitled to access their personal information as a way to request rectification or deletion of their personal data. They’re also entitled to make a complaint under this right and be notified about the safeguards put in place if their data is transferred to a third-party organisation.
3. **Right to rectification**: Users or an individual have the right to rectify incorrect data submitted to organisations. It is fairly straightforward, if the user realises that their data is incorrect or invalid then they ask for a rectification request and the organisation must comply with it.
4. **Right to erasure**: Users or an individual can submit a request to have their data to be erased. This right is applicable in certain circumstances. If the purpose for which organisation has collected data is no longer required or necessary, then the user can request that organisation to have their data erased. For example, when a newsletter subscriber doesn’t intend to receive offers or updates in their mailbox then the newsletter company must erase the person’s data.
5. **Right to restrict processing**: Users or an individual can ask for restricting the processing or use of their data. Similar to Right to erasure, right to restrict processing is nor absolute and applies only in certain circumstances. Similar to the above example, the newsletter can stop its subscription to the subscriber but can keep their data.
6. **Right to data portability**: Users or an individual has the right under GDPR to obtain and use their personal data for their own purposes across different services. Organisations can be asked by users to extract and transfer their data (commonly in CSV files) to other organisations directly if required.
7. **Right to object**: Users or an individual has right to object under GDPR to their data being processed for direct marketing and processing based on a legitimate interest based on the user having grounds to object. Organisations must immediately stop processing the user’s data when they receive such notice.
8. **Rights related to automated decision-making inducing profiling**: Users or an individual have the right to object to an assessment being made by an automated machine where the outcome of the assessment may have a legal impact on the user. Users can opt for having their assessment assessed by a human rather than a machine. (Sarah El-Atm, 2018)

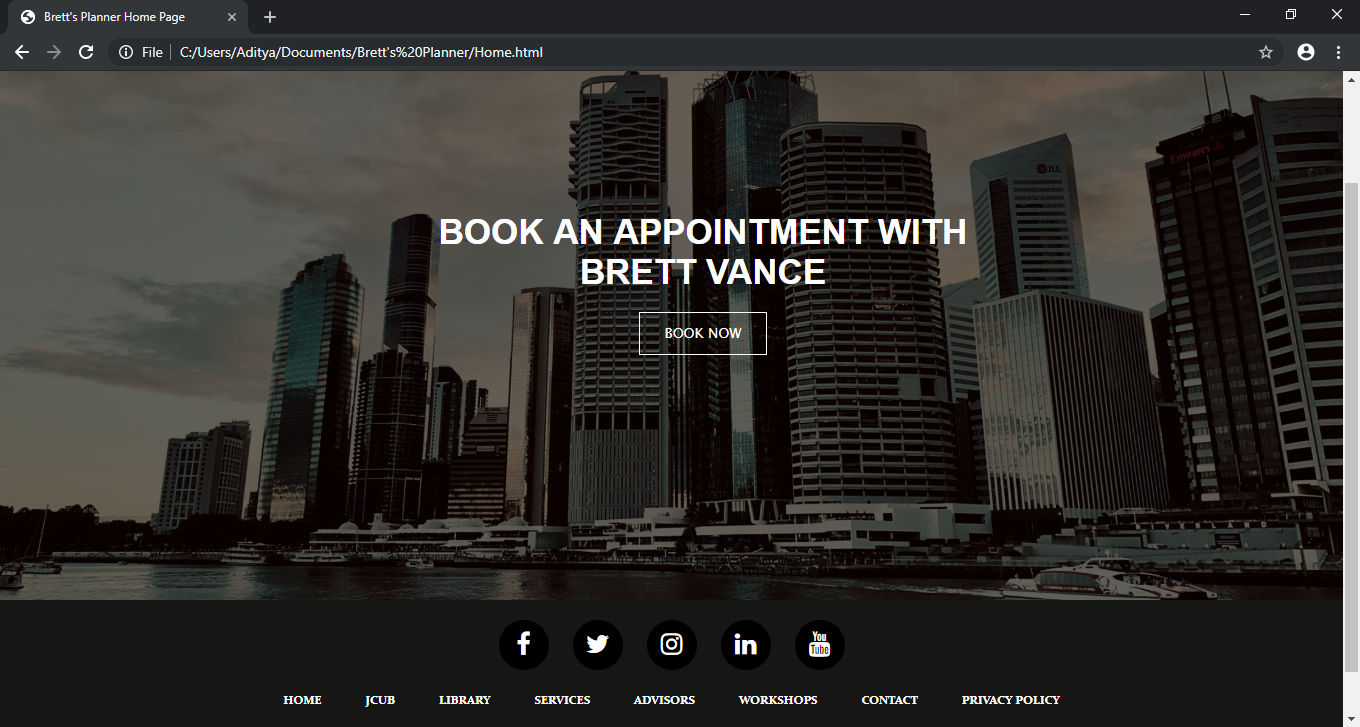
**Data Privacy Laws pertaining to their Region**

|  |  |
| --- | --- |
| Country | Data Privacy Law In compliance |
| European Union | General Data Protection Regulation (GDPR) |
| United Kingdom | Data Protection Act 2018 |
| Australia | Privacy Act 1988 |
| India | Personal Data Protection Bill 2018 (draft) |
| United States | The California Online Protection Act (CalOPPA). Regulated by FTC. |
| Canada | Personal Information Protection and Electronic Data Act (PIPEDA) |
| Japan | The Personal Information Protection Act |
| Switzerland | Federal Act on Data Protection |
| Germany | Federal Data Protection Act 2001 |

(Privacy Policies, 2019)

**Privacy Policy in Brett’s Planner**

The privacy policy of Brett’s Planner is located in the footer of the website. The website will need the users (students) to submit their information such as first and last name, student ID, student email ID, contact number and their purpose of visiting Mr. Brett Vance for booking an appointment through the website. The privacy policy protects this student information from being used for unintended purposes. This privacy policy is created using the Privacy Policy generator on <https://www.privacypolicies.com/> for free which complies with the Australian Privacy Act 1988 and follows the Australian Privacy Principles.



**Brett’s Planner Privacy Policy (as displayed on website) -**

**Privacy Policy**

Effective date: May 22, 2019

**Brett's Planner** ("us", "we", or "our") operates the http://portal.ictatjcub.com/Home.html website (hereinafter referred to as the "Service").

This page informs you of our policies regarding the collection, use, and disclosure of personal data when you use our Service and the choices you have associated with that data. Our Privacy Policy for Brett's Planner is created with the help of the [PrivacyPolicies.com Privacy Policy Generator](https://www.privacypolicies.com/free-privacy-policy-generator/).

We use your data to provide and improve the Service. By using the Service, you agree to the collection and use of information in accordance with this policy. Unless otherwise defined in this Privacy Policy, the terms used in this Privacy Policy have the same meanings as in our Terms and Conditions, accessible from <http://portal.ictatjcub.com/Home.html>

**Information Collection and Use**

We collect several different types of information for various purposes to provide and improve our Service to you.

**Types of Data Collected**

**Personal Data**

While using our Service, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you ("Personal Data"). Personally, identifiable information may include, but is not limited to:

* Email address
* First name and last name
* Phone number
* Cookies and Usage Data

**Usage Data**

We may also collect information on how the Service is accessed and used ("Usage Data"). This Usage Data may include information such as your computer's Internet Protocol address (e.g. IP address), browser type, browser version, the pages of our Service that you visit, the time and date of your visit, the time spent on those pages, unique device identifiers and other diagnostic data.

**Tracking & Cookies Data**

We use cookies and similar tracking technologies to track the activity on our Service and hold certain information.

Cookies are files with small amount of data which may include an anonymous unique identifier. Cookies are sent to your browser from a website and stored on your device. Tracking technologies also used are beacons, tags, and scripts to collect and track information and to improve and analyze our Service.

You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Service. You can learn more how to manage cookies in the [Browser Cookies Guide](https://privacypolicies.com/blog/how-to-delete-cookies/).

Examples of Cookies we use:

* **Session Cookies.** We use Session Cookies to operate our Service.
* **Preference Cookies.** We use Preference Cookies to remember your preferences and various settings.
* **Security Cookies.** We use Security Cookies for security purposes.

**Use of Data**

Brett's Planner uses the collected data for various purposes:

* To provide and maintain the Service
* To notify you about changes to our Service
* To allow you to participate in interactive features of our Service when you choose to do so
* To provide customer care and support
* To provide analysis or valuable information so that we can improve the Service
* To monitor the usage of the Service
* To detect, prevent and address technical issues

**Transfer of Data**

Your information, including Personal Data, may be transferred to — and maintained on — computers located outside of your state, province, country or other governmental jurisdiction where the data protection laws may differ than those from your jurisdiction.

If you are located outside Australia and choose to provide information to us, please note that we transfer the data, including Personal Data, to Australia and process it there.

Your consent to this Privacy Policy followed by your submission of such information represents your agreement to that transfer.

Brett's Planner will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy and no transfer of your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of your data and other personal information.

**Disclosure of Data**

**Legal Requirements**

Brett's Planner may disclose your Personal Data in the good faith belief that such action is necessary to:

* To comply with a legal obligation
* To protect and defend the rights or property of Brett's Planner
* To prevent or investigate possible wrongdoing in connection with the Service
* To protect the personal safety of users of the Service or the public
* To protect against legal liability

**Security of Data**

The security of your data is important to us but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure. While we strive to use commercially acceptable means to protect your Personal Data, we cannot guarantee its absolute security.

**Service Providers**

We may employ third party companies and individuals to facilitate our Service ("Service Providers"), to provide the Service on our behalf, to perform Service-related services or to assist us in analyzing how our Service is used.

These third parties have access to your Personal Data only to perform these tasks on our behalf and are obligated not to disclose or use it for any other purpose.

**Links to Other Sites**

Our Service may contain links to other sites that are not operated by us. If you click on a third-party link, you will be directed to that third party's site. We strongly advise you to review the Privacy Policy of every site you visit.

We have no control over and assume no responsibility for the content, privacy policies or practices of any third-party sites or services.

**Children's Privacy**

Our Service does not address anyone under the age of 18 ("Children").

We do not knowingly collect personally identifiable information from anyone under the age of 18. If you are a parent or guardian and you are aware that your Children has provided us with Personal Data, please contact us. If we become aware that we have collected Personal Data from children without verification of parental consent, we take steps to remove that information from our servers.

**Changes to This Privacy Policy**

We may update our Privacy Policy from time to time. We will notify you of any changes by posting the new Privacy Policy on this page.

We will let you know via email and/or a prominent notice on our Service, prior to the change becoming effective and update the "effective date" at the top of this Privacy Policy.

You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.

**Contact Us**

If you have any questions about this Privacy Policy, please contact us:

* By mail: adityawalunj@gmail.com

**Conclusion –**

Privacy Policies are mandatory by law. A number of countries throughout the world require their organisational websites or app to have a Privacy Policy if the website or app collects or uses personal information of the citizens. Privacy policy have become an essential requirement for e-commerce websites and other services agreements. Even common third-party web and app services like Google Analytics or Apple’s App Store require organisations to include a Privacy Policy before using their services. For any business or organisations collecting personal or sensitive information, maintaining the customer’s or user’s privacy is extremely important. Privacy policies are designed to shield companies and organisations from lawsuits. (Pegarella, 2017)

Over the past few years, internet spam and security leaks have increasingly caused problems for major organisations as well as its users and customers. Internet users all over the world are concerned having their personal information scattered around the web. Users are concerned with who sees and uses their information when they’re visiting a website or using a mobile application. The inclusion of Privacy Policy in websites and mobile applications has become an important factor. It is also important to keep an update on Privacy Policies as company policies may change overtime. It ensures users that their identifying information will not be shared, sold or misused in any marketing efforts directly or indirectly.

# References

Balaji, S. (2018, August 3). *India Finally Has A Data Privacy Framework -- What Does It Mean For Its Billion-Dollar Tech Industry?* Retrieved from Forbes: https://www.forbes.com/sites/sindhujabalaji/2018/08/03/india-finally-has-a-data-privacy-framework-what-does-it-mean-for-its-billion-dollar-tech-industry/#6fe37dda70fe

OAIC. (2019). *Privacy Law*. Retrieved from OAIC: https://www.oaic.gov.au/privacy-law/

Palmer, D. (2019, May 17). *What is GDPR? Everything you need to know about the new general data protection regulations*. Retrieved from ZDNet: https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/

Pegarella, S. (2017, August 01). *4 Reasons You Need a Privacy Policy*. Retrieved from Terms feed: https://www.termsfeed.com/blog/top-4-reasons-you-need-privacy-policy/

Privacy Policies. (2019, February 05). *What’s Data Privacy Law In Your Country?* Retrieved from Privacy Policies: https://www.privacypolicies.com/blog/privacy-law-by-country/#australia

Rouse, M. (2013, October). *Privacy Policy.* Retrieved from Tech Target: https://whatis.techtarget.com/definition/privacy-policy

Sarah El-Atm, R. B. (2018, May 22). *GDPR: What it means for Australian businesses.* Retrieved from August: https://www.august.com.au/blog/gdpr-what-it-means-for-australian-businesses/

TermsFeed. (2016, October 23). *Privacy Policy for United States.* Retrieved from Terms Feed: https://www.termsfeed.com/blog/privacy-policy-united-states/

Unknown. (2019, March 11). *Sample Privacy Policy Template.* Retrieved from Free Privacy Policy: https://www.freeprivacypolicy.com/blog/sample-privacy-policy-template/