INCOGNIA™

Delivering **Privacy by Design**

Introduction

Data protection laws around the world require organizations to implement technical and administrative measures to protect user privacy. But what does that mean in practice? How does a company implement each of the seven fundamental principles of Privacy by Design through technical and organizational measures? In this white paper we answer these questions using Incognia as a model of the implementation of Privacy by Design.

Authors

Raissa Moury
Head of Data Privacy, Incognia

Lara Ferraz
Data Privacy Associate, Incognia

Designer

Evandro Truzzi

Incognia
Palo Alto, July, 2020.

What is Privacy by Design?

What is Privacy by Design?

Privacy by Design is a privacy-first approach to systems engineering. It is comprised of 7 fundamental principles, which aim to ensure that privacy is built into products and services by default. The idea was developed by Ann Cavoukian, an expert in data privacy and protection and the former Information and Privacy Commissioner for the province of Ontario, Canada, between 1997 and 2014. She published this framework in **the article entitled, "Privacy by Design: the 7 fundamental principles".**

These principles help organizations secure personal data and ensure that privacy is embedded into every tool, process, system, product and service of any organization. Thanks to these principles, technological development and innovation can be guaranteed while human rights and fundamental freedoms are respected.

At Incognia, we view ensuring the privacy of location data as paramount. Our number one company value is to respect and put user privacy first.

Collecting, storing and working with location data raises important considerations regarding user privacy.

Incognia follows the 7 fundamental principles of Privacy by Design to ensure that privacy is built into its products by default, rather than as an afterthought or compliance checkbox.

The 7 fundamental principles of Privacy by Design

01 Principle

Proactive not Reactive; Preventive not Remedial

Privacy by Design, or PbD, aims to take a proactive and preventative approach to privacy. PbD means not waiting for privacy violations to occur before acting, on the contrary, it aims to prevent them from happening in the first place. This should be done by taking both technical and organizational measures, as detailed in the next section.

Organizational Measure

Ensure that your organization's directors and shareholders are committed to upholding the highest standards of privacy. This means not just complying with data protection regulations, but also proactively preventing any business practice or decision that could negatively impact the privacy of the users of your products and services.

Technical Measure

Employ the best preventive methods so that privacy issues are identified and corrected at the design stage, before any product is developed and launched. The goal is to systematically evaluate and implement alternatives that are both innovative, and more protective of privacy.

Incognia Implementation

Privacy by Design
Principle 01

At Incognia, our number one company value is to respect and put user privacy first. Privacy is the foundation for our decision making. We have established an organizational culture focused on respecting and protecting user privacy. We view compliance with government regulations as a legal obligation but recognize that abiding by regulations does not necessarily guarantee user privacy. As a company we are willing to adopt measures that go far beyond compliance to ensure user privacy.

Our technology is designed to protect people's identity and prevent access to information that can directly track or identify an individual. We focus on encrypting and protecting the location data we collect and intentionally do not collect additional PII. This means that Incognia does not collect unique static device identifiers (such as IMEI and MAC), associated accounts (e-mail and telephone), civil identification data (name and social security number), as well as sensitive data – information that reveals ethnicity, religion, political opinion, religious, philosophical, political or union entities membership or data regarding health, sex life, genetics, and biometrics.

It is incredibly difficult to fully anonymize a precise location dataset, but we get pretty close. It is important to identify which data is capable of re-identifying a user and apply cryptographic techniques, like encryption and hash, to it. Our goal is to transform location data into an unreadable version of itself so it can still be used, with techniques like zero knowledge proof, but can't be read without an encryption key, or in certain cases, not at all. Other techniques, including probabilistic set structure, differential privacy, and k-anonymity, bring the data closer to full anonymization, making it nearly impossible to identify an individual user from the location data set.

02 Principle

Privacy by default

Personal data should be automatically protected in any information technology (IT) system or business practice so that individuals do not need to make any efforts to have their privacy guaranteed. As such, no action is required on the part of the individual to protect his/her privacy - it is built into the system by default. This can be done by means of technical and organizational measures, according to the following examples:

Organizational Measure

Specify the purpose for the collection, use, storage and sharing of personal data even before collecting it. This principle of PbD is therefore strictly related to the principle of purpose, provided for in Article 6, (I), of the GDPR. If there is no legitimate purpose for the processing of the data, it should be avoided by default.

Technical measures

(i)

Limit the collection only to the information strictly necessary for the specific purposes and related to the service or product utilized by the user. This measure is related to the principle of necessity, established by Article 6, (III), of the GDPR.

(ii)

Collect the least amount of information possible and do the utmost not to identify the data subject individually, collecting only the data that is relevant and essential to the fulfillment of your legitimate purposes. This practice is directly related to the principle of minimization provided for in Article 5, 1, c of the GDPR.

(iii)

Limit the use, storage and disclosure of personal data to the relevant purposes identified and only process personal data in a lawful, fair and transparent way.

Incognia Implementation

Privacy by Design
Principle 02

We clearly specify the purpose of the processing of personal data in our Privacy Policy and the processing operation should be lawful, fair and transparent. This consent is required prior to data collection - therefore, there is no collection without consent.

It is also worth mentioning that Incognia meets the guarantee of effectiveness of the principle of necessity (article 6, item III, of GDPR) or minimization (article 5, item 1, c, of GDPR) on behalf of our clients. By using Incognia's technology, partner apps do not need to process location data - meeting the principle of necessity and minimization - and can focus on their core business, benefitting from Incognia's expertise to process location data securely and with a guarantee of privacy.

Lastly, we collect as little information as possible and make every reasonable effort not to identify the data subject individually, using only the data that is relevant and essential to the length of the legitimate purposes authorized by the data holder. Incognia employs techniques that limit data collection to an average of 2.5 daily visits per user, and only if the user activates and keeps his/her geolocation on. Incognia also blocks visits to sensitive sites - such as religious temples, hospitals and day care centers. Therefore, we minimize data processing, ensuring that there is no intrusion or individual tracking. Personal data is stored only for the time necessary to fulfill the stated purposes and then safely deleted. These practices are, by default, the highest privacy protection standards.

03 Principle

Design-Embedded Privacy

Privacy should be an essential component of the functionality of a product or service made available to society and should be incorporated into technologies in a holistic, secure and creative manner. This can be done in the following manner:

Organizational Measure

Implementing a systematic approach to Privacy by Design based on recognized standards and frameworks, subject to external reviews and audits. It is important to carry out, whenever possible, detailed privacy impact and risk assessments with clear documentation of the PbD techniques employed, measures taken to mitigate risks, using objective metrics to assess impact and risk to privacy.

Technical measures

Incorporate privacy into product and service design, minimizing the impact of technology on people's privacy, so that privacy settings are not easily degraded through use, misconfiguration or system error.

INCOGNIA™

Incognia Implementation

Privacy by Design
Principle 03

We incorporate privacy into our information technologies, operations and architecture in a holistic, integrated and creative way, facilitating the creation of customized and humanized experiences for application users. This allows individuals to be assisted in new account creation and automation of the registration process, without identifying people and with full protection of their identity. We know that incorporating privacy often means reinventing existing options, because the alternatives are not acceptable. Our team works every day to solve this challenge. As a result, privacy has become an essential component of the core functionality of Incognia's products. Privacy is an intrinsic part of the system, without diminishing its functionality - exactly as Ann Cavoukian has stated, because Incognia is able to deliver relevant results for individuals and society while maintaining the highest standards of privacy and data protection

04 Principle

Complete Functionality

Privacy by Design seeks to accommodate all legitimate goals and interests in a positive way, with “twofold benefits” for individuals and the society. Therefore, it rejects old-fashioned approaches that place privacy as a zero-profit calculation and highlights that by setting legitimate goals, it is possible to innovate while respecting privacy, which will result in a positive outcome. This principle can be put into practice by means of the following measures:

Organizational Measure

Accommodate all legitimate and positive interests, avoiding false dichotomies, such as privacy vs. security, demonstrating that it is possible and much more desirable to have both. It’s important to record: (i) the decisions and processes that were rejected for having a zero-sum outcome; (ii) how it was possible to meet legitimate objectives that are not related to privacy, and (iii) what solutions were found to meet these objectives with respect to privacy.

Technical measures

Develop innovative technologies that achieve real positive outcomes, where multiple interests beyond privacy can be met. Ann Cavoukian stresses that organizations that manage to overcome zero-sum choices without compromising the products and services functionality, achieved global leadership in privacy.

Incognia Implementation

Privacy by Design
Principle 04

We embrace this principle and reject any kind of false dichotomy such as “privacy vs. security”, or “privacy vs. revenue”, because our technology is proof that it is possible to guarantee our customers’ goals, fostering economic development and innovation, the goals of the company itself, and above all, delivering the benefits of technology to people with respect to their individual rights and freedoms, by incorporating privacy into our business model.

05 Principle

End-to-end security and protection throughout the data life cycle

Privacy by Design ensures the secure management of information throughout the data life cycle. There should be no gap in data protection or accountability. This is something that can be guaranteed by implementing the measures below:

Organizational Measure

Accept responsibility for the security of personal data throughout its life cycle, adopting a strong Information Security policy, as well as the best available techniques on the market and the standards developed by recognized organizations.

Technical measures

Ensure the confidentiality, integrity and availability of personal data throughout their life cycle, while using, among other techniques, strong encryption, appropriate methods of access control and recording operations involving personal data, and secure deletion.

Incognia Implementation

Privacy by Design
Principle 05

We base our approach on the assumption that privacy is not possible without security, and implement the best practices to ensure the confidentiality, integrity and availability of personal data throughout its life cycle.

Among other methods used at Incognia we apply an advanced technique to pseudonymize IDs and replaced with encrypted and hashed data, as described in the Privacy Policy. The hashed and encrypted IDs are sufficient to supply Incognia services and do not allow the identification of data holders. Thus, in the event of any unauthorized access to the hashed and encrypted IDs, it will not be possible for the third party to directly associate any user with such data.

Incognia also applies advanced technique to pseudonymize location data. Our goal is to transform location data into an unreadable version of itself so it can still be used, with techniques like zero knowledge proof, but can't be read without an encryption key, or in certain cases, not at all. Other techniques, including probabilistic set structure, differential privacy, and k-anonymity, bring the data closer to full anonymization, making it nearly impossible to identify an individual user from the location data set

Thus, in the event of any unauthorized access to the hashed and encrypted IDs, it will not be possible for the third party to directly associate any user with such data.

06 Principle

Visibility and transparency

In PbD, transparency, diligence and compliance are fundamental in establishing accountability and trust, assuring the interested parties that the organization is operating in accordance with its statements and objectives and that its promises can be verified. This principle can be put into practice as follows:

Organizational Measure

Document and make available policiesand procedures related to privacy and provide a communication channel to facilitate petitions from holders, partners and public authorities. It is also important to establish a procedure for auditing third parties whenever the transfer of personal data to them is necessary, to verify that they employ the appropriate security requirements and to establish contractual data protection clauses.

Technical measures

Establish technical measures capable of continuously monitoring and evaluating compliance with data protection policies and proceduresare.

INCOGNIA™

Incognia Implementation

Privacy by Design
Principle 06

We take pride in transparency, diligence and compliance. Our systems are subject to independent verification and we have a team focused exclusively on data protection, which counts on the participation of specialized lawyers to ensure that all current regulations and legal obligations are being met in practice with continuous monitoring and improvement.

We keep information on policies and practices related to the protection of personal data at the full and immediate disposal of our employees, customers, partners, authorities and data holders, and we provide a communication channel through the e-mail address.

07 Principle

Respect for user privacy

Above all, Privacy by Design requires organizations to value the interests of the individuals, keeping the user in control of his/her data. The best PbD results are those designed to meet the needs of the data holders by putting them first. The measures below explain how this can be done.

Organizational Measure

Enable data holders to actively manage their personal data, avoiding abuse and improper use of their data

Technical measures

Establish strong privacy standards, appropriate notices and user-friendly interfaces that allow the data holder to properly exercise all his/her rights ensured by law, and that give them absolute control over his/her personal data.

INCOGNIA™

Incognia Implementation

Privacy by Design
Principle 07

We use strong privacy standards, far above the standards adopted by other companies in the industry.

We design for privacy looking always to the individual's interests. We believe that the value of technology is to serve humanity and people should not give up their privacy to have convenience, so we respect and put user privacy first. We don't want to know who our user is and we do not collect the special categories of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data and biometric data processed for the purpose of uniquely identifying a natural person, data concerning a natural person's sex life or sexual orientation, avoiding any kind of bias on our algorithms.

Conclusion

The 7 fundamental principles that shape Privacy by Design must be present in all technology, processes, culture and governance of a company. In other words, it must be an intrinsic part of its DNA.

At this time of growing appreciation of the human right to privacy and growing surveillance in data protection matters, organizations that wish to gain the trust of their consumers and partners, in addition to standing out from their competitors, must invest in the implementation of technical and organizational measures that cover all aspects of PbD.

Incognia puts user privacy first and has built Privacy by Design into the fabric of the company and its products.

About this e-book

This e-Book is part of Incognia's initiatives to promote data protection and privacy.

We put user privacy first.

Incognia is a private identity company that enables the use of anonymized location behavioral data to increase account security, reduce fraud, and deliver private location context aware services.

Companies with mobile apps and connected devices use Incognia for frictionless user ID verification, dynamic adaptive authentication, risk assessment and fraud detection, all while protecting user privacy.

We are headquartered in Palo Alto, with teams in the San Francisco Bay Area, New York, and Brazil.

Learn more about our solutions ⟶