Data Protection By Design

GUIDE

Co-Creation Hub

THRIVACY

TECH HIVE ADVISORY

Safe Online by CcHUB

SCENARIO

DISAP AIR is a promising Nigerian startup that recently raised $27 million in its Series C funding. It is based in Lagos and provides an innovative solution to the city's notorious traffic congestion through provision of transportation by means of a specially designed "pod" that cuts down travel time. Like any other business looking to harness the strategic advantages of big data, DISAP AIR uses data-driven decision making to fuel growth and to ensure seamless user experience. In providing the service, it collects the personal data of its users to determine service preference and to personalize offerings. The personal data collected and processed includes name, mobile phone number, location data, biometric data and health data. The users' data is stored without time limits. The application used by users to make secure a seat and manage bookings requires permission to listen to calls and read messages on users' devices. Their watchword is "we know where you are, we know where you are going." Urban dwellers love the convenience brought forth by DISAP AIR's solution, on average there are 10,000 new users every month. DISAP AIR recognizes the golden opportunity that this is, thus makes money by selling the data it collects to advertisers and media content providers. The privacy notice of DISAP AIR both on the mobile application and web site is just a 6 line draft alluding to how they take privacy seriously; it is silent on the startup's data collection, processing and sharing practices, it says nothing about the cookies and web beacons embedded on their applications, it also does not provide a channel through which a user could make an enquiry about their personal data.

DATA PROTECTION BY DESIGN AND DEFAULT

The General Data Protection Regulation ("GDPR") requires that a data controller put in place appropriate technical and organisational measures to implement the data protection principles in order to meet the requirements of the regulation and to protect the rights of the data subject. The measures are to be implemented both at the time of the determination of the means for processing and at the time of the processing itself. This is data protection by design and default. Data protection by design and default entails embedding data protection into the design of technology, systems and practices and throughout the lifecycle, such that data protection is considered from the beginning, rather as an afterthought.

DISAP AIR delivers its solution in Nigeria, therefore processes the personal data of individuals resident in Nigeria. DISAP AIR is subject to the data protection legal framework in Nigeria being the Nigeria Data Protection Regulation ("NDPR"). The NDPR just like the GDPR seeks to protect the rights of individuals as it relates to their personal data. Whilst the NDPR makes provision for data protection principles and requires adherence to the principles in the processing of personal data by controllers and processors, the regulation is silent on the data protection by design and default; it has no express provision similar or with the same effect as Article 25 of the GDPR.

Even though the legislative framework applicable to DISAP AIR does not make implementing privacy by design and default an express legal requirement, data protection by design and default is an effective mechanism for upholding the principles of data protection. By implementing a privacy-first best practice framework DISAP AIR would guarantee only personal data that is necessary for a specific purpose is collected, only personal data that is relevant to the original data collection purpose can be processed, personal data that is no longer needed is deleted and data subjects can exercise their rights accordingly. Compliance with the NDPR then becomes less burdensome since by design and default, the data protection principles in the regulation would be adhered to.

IMPLEMENTATION OF DATA PROTECTION BY DESIGN AND DEFAULT BY DISAP AIR

In light of the scenario described above with respect to DISAP AIR's solution and its processes, below is an illustration of how the implementation of the data protection by design principles would positively impact DISAP AIR's attitude towards the protection of personal data:

Proactive not Reactive; Preventative not Remedial
The data protection by design approach anticipates and prevents privacy invasive events before they happen. It aims to prevent data breaches from occurring. Through this principle DISAP AIR would have a clear commitment to set and enforce high standards of privacy. DISAP AIR would go beyond claiming to respect users' privacy to actually establishing methods to recognize poor privacy designs, anticipate poor privacy practices and outcomes, and correct any negative impacts, well before they occur in proactive, systematic, and innovative ways.

Privacy as a Default
This principle seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given system or business practice. No action is required on the part of the individual to protect their privacy – it is built into the system, by default. With privacy as a default DISAP AIR to achieve purpose specification, collection limitation, data minimization, and use, retention and disclosure limitation. DISAP AIR would only process users' personal data the purpose that was presented during collection; it would not be used for marketing unbeknown to users. DISAP AIR would limit the collection of sensitive data and data that is not critical to their service delivery like health data.

Privacy embedded into design
This principle is concerned with incorporating measures that ensure privacy and data protection in the design and architecture of systems and business practices such that data protection becomes an essential component of the core functionality being delivered. In this way data protection becomes integral to the system without diminishing functionality. Through this principle, DISAP AIR would rethink the permissions required by their application, the manner in which their application operates as well as their identity management and access control methods. A data protection impact assessment should have been carried out by DISAP AIR to assess the impact the envisaged software or processing operation may have on the individual's right to privacy and data protection.

Full Functionality – Positive-Sum, not Zero-Sum
Data protection by design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a zero-sum approach, where trade-offs are made. The approach is such that all legitimate interests should co-exist harmoniously and that when embedding privacy into a given technology, process, or system, it should be done in such a way that full functionality is not impaired, and to the greatest extent possible, that all requirements are optimized.

End-to-End Security – Lifecycle Protection
Without strong security, there can be no privacy. Privacy must be continuously protected across the entire domain and throughout the life-cycle of the data in question. This principle would help DISAP AIR achieve the 'security' principle of data

protection. DISAP AIR has to implement applied security standards that assure the confidentiality, integrity and availability of personal data throughout its lifecycle including, inter alia, methods of secure destruction, appropriate encryption, and strong access control and logging methods.

Visibility and Transparency

This principle is critical to the achievement of the transparency and accountability data protection principle. It is at the center of trust between all stakeholders. Adherence to this principle would encourage DISAP AIR to amend their privacy policy, to have it communicate its data protection practices better than it currently does. The privacy policy would be more detailed and open about how DISAP AIR handles personal data.

Respect for User Privacy

This principle is concerned with the following fair information practices: consent, accuracy, access and compliance. Through this principle DISAP AIR would give effect to the data subject rights set out in the NDPR. The start-up would get consent where necessary, it would keep the data accurate, let the data subject have access to their data and establish mechanisms for complaints and redress for data subjects.

SECURITY BY DESIGN AND DEFAULT

The success of any data protection program is tied to the implementation of standard security designs and controls. This is so as data protection is inherently a two-pronged idea involving the Law and Information Security.

Considering and building security into every phase of a project like DISAP Air's will save millions in penalties and sanctions from data breaches under the NDPR as the company can identify well beforehand, the various security standards, design architecture and controls to implement at each stage of the project to forestall such threats as database dumping, unauthorized access, theft or modification of confidential data, insider threats and compromises, etc, all of which have severe ramifications under the Nigerian Data Protection Regulation.

Security by design and default occurs in three key phases: Pre-Development, Development and Post-Development.

Pre-Development

The considerations and activities in the Pre-development phase includes all such planning and preparation before the coding or development of the software. This is an elaborate phase involving every stakeholder (from IT to top management) and includes defining the project goal and objectives, identifying project personnel, agreeing on techniques, rules and standards, etc. This is not entirely different from the Planning phase of a Software Development Lifecycle, however it differs in that it has strong considerations for data protection and the rights of data subjects across the decision-making processes.

Other Pre-development activities include:

Onboarding and Training: Onboarding and training is a series of activities that both teaches and addresses how and why details like the tools and technologies to be used, the types and choices of configuration, protocols and frameworks to employ, third-party licenses, plugins and extensions, access control, encryption, etc, all impact the overall success of the project in terms of data protection and ensuring the privacy of users/customers. Secure software development is still a relatively new talking point for many software developers, which is why at the outset of development, an organisation like DISAP Air must properly on-board and train the developers, engineers and designers and all stakeholders involved in the building, maintenance and administration of the software.

Encryption: Encryption is at the heart of security. Among other things, it ensures the confidentiality of data and information, which is key in data protection regulations. Alongside other IT decisions (such as what development framework to use), deciding on encryption algorithms and standards well before actual development will prevent future bottlenecks such as compatibility issues.

Several encryption algorithms exist, each serving a slightly different purpose.

Below are some of the most secure (and recommended) encryption and hashing algorithms/functions:

- ***AES** – Also known as Advanced Encryption Standard, is a popularly used algorithm. AES replaced Data Encryption Standard, DES, and became a standard encryption technique adopted by the US government in 2002.*

  By design, AES is a block-cipher consisting of 128 bits or 192 bits or 256 bits. A block cipher encrypts data one block at a time. Though 128 bits are strong and efficient, 256 bits are used for high-grade encryption. It is a symmetric algorithm which uses a single private key for encryption and decryption.

- ***3DES** – The Triple Data Encryption Standard is also a block-cipher based on the older Data Encryption Standard, DES, and uses the 56-bit key and has a 64-bit block size. 3DES is a symmetric key encryption and provides three times the encryption of DES.*

  It is used by several financial institutions and a number of industries to keep data secure. It is a more robust algorithm, but since this does a three times encryption, it is slightly slow in performance.

- ***Blowfish** – This is yet another algorithm which was designed initially to replace DES. A further well-known version of this is Twofish. This is a symmetric cipher which uses 64-bit blocks and encrypts them individually. It gained immense popularity owing to its speed and effectiveness. It is license-free and non-patented and used in several software categories such as e-commerce to secure payment, password management and many more. Blowfish is one of the most flexible encryption algorithms for its array of applications.*

- ***Twofish** – This is based on Blowfish and is a block-cipher. It has a block size of 128 bits and 256 bits and can perform equally well on smaller CPU or hardware. It utilizes several rounds of encryption to convert plain text to cipher text. However, unlike AES, irrespective of the key size, this always has 16 rounds.*

- ***RSA** – RSA is a very popular algorithm for encrypting data over an insecure network like the internet. It uses asymmetric public key encryption. It uses two different but mathematically linked keys for encryption and decryption. In this, a public key is used for encryption and a private key is used for decryption. As a thumb rule, the mathematically linked keys for encryption and decryption. In this, a public key is used for encryption and a private key is used for decryption. As a thumb rule, the public key can be shared with others, but the private key should be kept secret. RSA is commonly used for encryption and digital signatures and by design has a very large key size and hence is fairly secure. RSA keys are 1024-bit or 2014-bit long. The only disadvantage of having long key size is, it is slower than other encryption algorithms.*

Hashing: Hashing is an algorithm performed on data such as a file or message to produce a number called a hash (also called a checksum). The hash is used to verify that data is not modified, tampered with, or corrupted. While encryption mostly ensures confidentiality, hashing ensures the integrity of data.

Below are some industry standard Hashing Algorithms:

- ***MD5*** *– Message Digest 5 (MD5) is a common algorithm that produces a 128-bit hash. Hashes are commonly shown in hexadecimal format instead of a stream of 1s and 0s. For example, an MD5 hash is displayed as 32 hexadecimal characters instead of 128 bits. Hexadecimal characters are composed of 4 bits and use the numbers 0 through 9 and the characters "A" through "F".*

- ***SHA*** *– Secure Hash Algorithm (SHA) is another hashing algorithm. There are several variations of SHA grouped into four families — SHA-0, SHA-1, SHA-2, and SHA-3:*

  - *SHA-0 is no longer in use.*
  - *SHA-1 is an updated version that creates 160-bit hashes. This is similar to the MD5 hash except that it creates 160-bit hashes instead of 128-bit hashes.*
  - *SHA-2 improved SHA-1 to overcome potential weaknesses. It has four versions:*

    - *SHA-256 creates 256-bit hashes*
    - *SHA-512 creates 512-bit hashes*
    - *SHA-224 (224-bit hashes)*
    - *SHA-384 (384-bit hashes) create truncated versions of SHA-256 and SHA- 512, respectively.*

  - *SHA-3 (previously known as Keccak) is an alternative to SHA-2. The United States National Security Agency (NSA) created SHA-1 and SHA-2. SHA-3 was created outside of the NSA. It can create hashes of the same size as SHA-2 (224 bits, 256 bits, 384 bits, and 512 bits).*

- ***HMAC*** *– Hash-based Message Authentication Code (HMAC) is another method used to provide integrity to data and is by far the strongest. An HMAC is a fixed-length string of bits similar to other hashing algorithms such as MD5 and SHA-1 (known as HMAC-MD5 and HMAC-SHA1). In addition, HMAC also uses a shared secret key to add some randomness to the result and only the sender and receiver know the secret key.*

Data Protection Impact Assessment: A data protection impact assessment is necessary for assessing the impact of a planned software or processing operation on the protection of personal data. Its goal is to ensure that the software does not infringe on the data subject's fundamental rights.

DPIA therefore checks that processing of data is lawful, fair, and transparent, and typically involves:

- *An end-to-end description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*
- *An assessment to justify the necessity and proportionality of the processing and the corresponding risks and/or infringements on the rights of the data subject; and,*
- *The planned measures for addressing the identified risks, including safeguards, security controls and mechanisms to ensure the protection of personal data and to demonstrate compliance with the data protection regulation.*

Development

This phase of the project involves the actual development of the software solution and incorporates strong security considerations, standards and frameworks in the software development lifecycle (thus known as the Security Development Lifecycle).

“Secure Coding” and “Testing” are the two major activities in this phase and includes standard software development, defining security requirements, implementing secure authentication and encryption, static and dynamic security testing (incorporating the OWASP Top 10), fuzz testing, and code and data protection compliance review.

Below are some industry-standard frameworks and resources for secure web and software development and testing

- Microsoft Security Development Lifecycle
  https://www.microsoft.com/en-us/securityengineering/sdl/practices
- ISO/IEC 270034
  https://www.iso27001security.com/html/27034.html
- OWASP Top 10
  https://owasp.org/www-project-top-ten/
- EDRI’s Ethical Web Development
  https://edri.org/ethical-web-dev/

Post-Development

Although much of the project work is done in the development phase, the activities pre and post shipping of the product in the post-development phase are most essential to compliance with data regulations. While only the software engineers, designers, product lead and testers are involved in the Development phase, everyone from management, administrators, security auditors/ethical hackers, engineers and end users are brought onboard for various validation purposes post-development.

Key activities here include:

Training Post-development training is essential and targets the every-day administrators of the product (such as call-center operatives, non-technical staff, etc). Training will equip the target group with vital knowledge on the secure handling of products and data. It will typically include how and where to store data, processing data, rights of data subject, responding to requests of data subjects, storing and sharing passwords, etc.

Security Risk Assessment Conducting a risk or threat assessment exercise is essential for identifying the various threat actors that may be interested in the project assets (personal data in this case) and the associated vulnerabilities and vectors that may aid this. It involves using risk mapping to provide an explicit view of the impact of each risk and the likelihood of their occurrence. This map (or matrix) will help the IT team to prioritize and mitigate threats and dial down on organisational risks according to set risk tolerance levels.

Vulnerability Assessment and Penetration Testing (VAPT) Vulnerability assessment and penetration testing is a vital activity post-design. Here, the product is tested for vulnerabilities or flaws which are then exploited by the tester as would an actual adversary or hacker.

The major aim of this activity is to quickly find exploitable vulnerabilities and remediate them before an attacker does.

In addition to data protection regulations (such as the NDPR), companies may have other mandatory regulatory standards they must comply with (depending on industry). A good VAPT program will ultimately lead to (or, at the minimum, provide a solid technical base for) compliance with regulatory standards, such as;

- *ISO/IEC 27001/27002 (Manufacturing, Transportation, Information Technology, etc)*
- *Payment Card Industry Data Security Standard -PCI DSS (Finance, Payment, Retail)*
- *Health Insurance Portability and Accountability Act -HIPAA (Health)*
- *National Institute of Standards and Technology (NIST) (Manufacturing, Health, Infrastructure and Engineering, Information Technology, etc)*
- *Control Objectives for Information and Related Technology -COBIT (Information Technology)*

Companies should employ the service of a Licensed Penetration Tester, a Certified Information Systems Auditor or related expertise for Vulnerability Assessment and Penetration Testing.

Data Loss Prevention Complying with data protection regulations will prove a difficult (almost impossible) undertaking without data loss prevention in place. Data Loss Prevention (DLP) is the practice of detecting and preventing data breaches and the conscious or accidental exfiltration or destruction of sensitive data using an array of techniques, principles and technologies.

A data loss prevention solution:

Secures data at rest

Secures data in motion

Secures data in use

Classifies data (thus identifies which data is sensitive and which is not)

Assigns roles/privilege to users (so that sensitive data is not accessed by those without the requisite privilege)

Prevents data leak

Below are some leading data loss prevention solution to consider;

- *Symantec DLP*
- *SolarWinds DLP*
- *Checkpoint DLP*
- *Forcepoint DLP*
- *Digital Guardian Endpoint DLP*
- *RSA*

Incident Response A successful cyber attack or data breach can very strongly affect a business, its clients/customers, resources and even brand value.

Incident Response is an organization's plan for responding to and managing a cyberattack with the aim of minimizing threat and/or damage and to recover as quickly as possible.

An organization should look to their "Computer Incident Response Team (CIRT)" to lead incident response efforts. This team should comprise experts from upper-level management, IT, information security, IT auditors when available, as well as any physical security staff that can aid when an incident includes direct contact to company systems. Incident response should also be supported by HR, legal, and PR or communications.

There are six key steps to a response plan enumerated below:

Preparation Developing policy and procedure to follow in the event of a cyber breach. This will include determining the exact composition of the response team and the triggers to alert internal partners. Key to this process is the effective training of all staff on ways to respond to a breach and the proper documentation process of the breach. Documentation of breaches must be compulsory and action taken to review at a later date.

Identification This is the process of detecting a breach and enabling a quick and focused response. IT security teams identify breaches using various threat intelligence streams, intrusion detection systems, and firewalls. Threat intelligence professionals analyze current cyber threat trends, common tactics used by specific groups, and keep your company one step ahead.

Containment One of the first steps after identification is to contain the damage and prevent further penetration. This can be accomplished by taking specific sub-networks offline and relying on system backups to maintain operations. Your company will likely remain in a state of emergency until the breach is contained.

Eradication This stage involves neutralizing the threat and restoring internal systems. This can involve secondary monitoring to ensure that affected systems are no longer vulnerable to subsequent attack.

Recovery Security teams need to validate that all affected systems are no longer compromised and can be returned to working condition. This also requires setting timelines to fully restore operations and continued monitoring for any abnormal network activity. At this stage, it becomes possible to calculate the cost of the breach and subsequent damage.

Incident Lessons One of the most important and often overlooked stages. During this stage, the incident response team and partners meet to determine how to improve future efforts. This can involve evaluating current policies and procedures, as well specific decisions the team made during the incident. Final analysis should be condensed into a report and used for future training. Forcepoint can help your team analyze previous incidents and help improve your response procedures. Protecting your organization requires a determined effort to constantly learn and harden your network against malicious actors.

RECOMMENDATIONS

Before the commencement of processing, an effort should be made to identify possible privacy-invasive aspects of a product or service. Adequate safeguards should be put in place to protect data subjects' rights. When building products, developers should utilise privacy-friendly tools and frameworks, disabling unsafe functions and modules, and regularly carrying out static code analysis and code review. In addition, the product should be tested to ascertain "whether data protection and security requirements are implemented properly." Prior to launching, an incident response plan should be established, and a full security review of the software should be carried out. Data protection by design is to be maintained throughout the lifecycle of product,

REFERENCES

Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Found at:
https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

A Guide to Privacy by Design by AEPD (Spanish Data Protection Authority). Found at
https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf

Software development with Data Protection by Design and by Default. Datatilsynet (Norwegian Data Protection Authority). Found at
https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?print=true

Data protection by design and default. Information Commissioner Office (ICO). Found at
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

Privacy by Design - The 7 Foundational Principles Found at:
https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf

Handbook on European data protection law. 2018 Edition. Published by European Union Agency for Fundamental Rights. Found at
https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

CONTACT

Co-Creation Hub Nigeria,
6th Floor,
294 Herbert Macaulay Way,
Sabo, Yaba, Lagos.

T: +234 (01) 295 0555
E: info@cchubnigeria.com
W: www.cchubnigeria.com

Tech Hive

T: (+234) 8087878783
E: contact@techhiveadvisory.org.ng
W: www.techhiveadvisory.org.ng

Thrivacy

T: +267 75 419 903
E: hello@thrivacy.co.bw
W: www.thrivacy.co.bw