Coralogix Development Lifecycle

Version 2.0

Version Control

Version	Developed by	Changes	Approved by	Date
1.0	Oded David	Initial Version		
2.0	BDO	Update according to ISO 27701		30/05/2020

Coralogix development lifecycle procedure:

1) Weekly management teams design sessions
2) Stories are sent to the R&D teams for grooming
3) Stories are broken into tasks by the team
4) The development is done within 3 weeks
5) Definition of done includes 70% automation tests coverage, security measurements, monitoring and stability
6) Each task is developed under a feature branch
7) Any code push triggers unit tests proprietary to the modified area in the software
8) A new feature triggers a pull request
9) The pull request is reviewed by the teammates
10) After approval - a build is created with the new version and ran through tests
11) A successful build is deployed to a staging environment
12) After formally approving the pull request the developer may push the pull request to the master branch
13) The updated code is delivered to staging.
14) After 24 hours in the staging environment, the new code is pushed to production.

15) Privacy by design

    - Privacy by Design means building privacy into the design, operation, and management of a specific system, business process, or design specification. It is based on adherence to the 7 Foundational Principles of Privacy by Design: (See Appendix A)

        - Proactive not reactive—preventative not remedial
        - Lead with privacy as the default setting
        - Embed privacy into design
        - Retain full functionality (positive-sum, not zero-sum)

- Ensure end-to-end security
- Maintain visibility and transparency—keep it open
- Respect user privacy—keep it user-centric

Appendix A: Privacy by Design (PBD) — 7 Foundational Principles

A.1. Proactive not Reactive; Preventative not Remedial

A.1.1. Anticipate, identify, and prevent invasive events before they occur. This means taking action before the fact, not after.

A.1.1.1. Whether applied to information technologies, organizational practices, physical design, or networked information ecosystems, PbD begins with explicit recognition of the value and benefits of proactively adopting strong privacy practices, early and consistently (for example, preventing (internal) data breaches from happening in the first place). This implies:

A.1.1.1.1. Commitment, at the highest levels, to set and enforce high standards of privacy − generally higher than those standards set by global laws and regulation.

A.1.1.1.2. A privacy commitment that is demonstrably shared throughout by user communities and stakeholders, in a culture of continuous improvement.

A.1.1.1.3. Established methods for recognizing poor privacy designs, anticipating poor privacy practices and outcomes, and correcting any negative impacts, well before they occur, using proactive, systematic, and innovative methods.

A.2. Privacy as the Default Setting

A.2.1. Ensure personal data is automatically protected in all IT systems or business practices, with no added action required by any individual.

A.2.2. The PBD principle, which can be viewed as Privacy by Default, is particularly informed by the following FIPs:

A.2.2.1. Purpose Specification: The purposes for which personal information is collected, used, retained and disclosed shall be communicated to the individual (data subject) at or before the time the information is collected. Specified purposes should be clear, limited and relevant to the circumstances.

A.2.2.2. Collection Limitation: The collection of personal information must be fair, lawful and limited to that which is necessary for the specified purposes.

A.2.2.3. Data Minimization: The collection of personally identifiable information should be kept to a strict minimum. The design of programs, information and communications technologies, and systems should begin with non-identifiable interactions and transactions as the default. Wherever possible, identifiability, observability, and linkability of personal information should be minimized.

A.2.2.4. Use, Retention, and Disclosure Limitation: The use, retention, and disclosure of personal information shall be limited to the relevant purposes identified to the individual, for which he or she has consented, except where otherwise required by law. Personal information shall be retained only as long as necessary to fulfill the stated purposes, and then be securely destroyed.

A.2.2.5. Where the need or use of personal information is unclear, there shall be a presumption of privacy, and the precautionary principle – the default settings shall be the most privacy protective – shall apply.

A.3. Embed Privacy into Design

A.3.1. Privacy measures should not be add-ons, but fully integrated components of the system.

A.3.2. Privacy must be embedded into technologies, operations, and information architectures in a holistic, integrative and creative way. Holistic, because additional, broader contexts must always be considered. Integrative, because all stakeholders and interests should be consulted. Creative, because embedding privacy sometimes means re-inventing existing choices because the alternatives are unacceptable.

A.3.2.1. A systemic, principled approach to embedding privacy should be adopted − one that relies upon accepted standards and frameworks that are amenable to external reviews and audits. All fair information practices should be applied with equal rigor, at every step in the design and operation.

A.3.2.2. Wherever possible, detailed privacy impact and risk assessments should be carried out and published, clearly documenting the privacy risks and all measures taken to mitigate those risks, including consideration of alternatives and the selection of metrics.

A.3.2.3. The privacy impacts of the resulting technology, operation or information architecture, and their uses, should be demonstrably minimized, and not easily degraded through use, misconfiguration or error.

A.4. Retain Full Functionality (Positive-Sum, Not Zero-Sum)

A.4.1. Privacy by Design employs a “win-win” approach to all legitimate system design goals. That is, both privacy and security are important, and no unnecessary trade-offs are required in achieving both.

A.4.2. Privacy by Design does not simply involve the making of declarations and commitments, it relates to satisfying all of an organization's legitimate objectives − not only its privacy goals. Privacy by Design is doubly enabling in nature, permitting full functionality − real, practical results and beneficial outcomes to be achieved for multiple parties.

A.4.2.1. When embedding privacy into a 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.

A.4.2.2. Privacy is often positioned in a zero-sum manner, as having to compete with other legitimate interests, design objectives, and technical capabilities, in a specific domain. Privacy by Design rejects such an approach, it embraces legitimate non-privacy objectives and accommodates them, in an innovative positive-sum way.

A.4.2.3. All interests and objectives must be clearly documented, preferred functions articulated, metrics agreed upon and applied, and trade-offs often rejected as being unnecessary, in favor of finding a solution that enables multi-functionality.

A.5. Ensure End-to-End Security

A.5.1. Data lifecycle security means all data should be securely retained when required, and destroyed when no longer required.

A.5.2. Privacy must be continuously protected, across the entire domain and throughout the life-cycle of the data in question. There should be no gaps in either protection or accountability. The "Security" principle has special relevance here because, at its essence, without strong security, there can be no privacy.

A.5.2.1. Security personnel must assume responsibility for the security of personal information (generally commensurate with the degree of sensitivity) throughout its entire lifecycle, consistent with standards that have been developed by recognized standards development bodies.

A.5.2.2. Applied security standards must 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.

A.6. Maintain Visibility and Transparency—Keep it Open

A.6.1. Assure stakeholders that business practices and technologies are operating according to objectives and subject to independent verification.

A.6.2. Visibility and transparency are essential to establishing accountability and trust. The PBD principle is a good parallel to Fair Information Practices in their entirety, but for auditing purposes, special emphasis may be placed on the following FIPs:

A.6.2.1. Accountability – The collection of personal information entails a duty of care for its protection. Responsibility for all privacy-related policies and procedures shall be documented and communicated as appropriate, and assigned to a specified individual. When transferring personal information to third parties, equivalent privacy protection through contractual or other means shall be secured.

A.6.2.2. Openness – Openness and transparency are key to accountability. Information about the policies and practices relating to the management of personal information shall be made readily available to individuals.

A.6.2.3. Compliance – Complaint and redress mechanisms should be established, and information communicated about them to individuals, including how to access the next level of appeal. Necessary steps to monitor, evaluate, and verify compliance with privacy policies and procedures should be taken.

A.7. Respect User Privacy—Keep It User-Centric

A.7.1. Keep things user-centric; individual privacy interests must be supported by strong privacy defaults, appropriate notice, and user-friendly options.

A.7.2. The best Privacy by Design results are usually those that are consciously designed around the interests and needs of individual users, who have the greatest vested interest in the management of their own personal data.

A.7.3. Empowering data subjects to play an active role in the management of their own data may be the single most effective check against abuses and misuses of privacy and personal data. Respect for User Privacy is supported by the following FIPs:

A.7.3.1. Consent – The individual's free and specific consent is required for the collection, use or disclosure of personal information, except where otherwise permitted by law. The greater the sensitivity of the data, the clearer and more specific the quality of the consent required. Consent may be withdrawn at a later date.

A.7.3.2. Accuracy – Personal information shall be as accurate, complete, and up-to-date as is necessary to fulfill the specified purposes.

A.7.3.3. Access – Individuals shall be provided access to their personal information and informed of its uses and disclosures. Individuals shall be able to challenge the accuracy and completeness of the information, and to have it amended as appropriate.

A.7.3.4. Compliance – Organizations must establish complaint and redress mechanisms, and communicate information about them to the public, including how to access the next level of appeal.

Ariel Assaraf
CEO