Università degli Studi di Bari “Aldo Moro”

Dipartimento di Informatica

Corso di laurea in Informatica

Tesi di laurea in

**INGEGNERIA DEL SOFTWARE**

Una Base di Conoscenza di Supporto allo Sviluppo Software Orientato alla Privacy

Relatori:

**Chiar.mo Prof. Danilo CAIVANO**

**Dott.ssa Vita Santa BARLETTA**

Laureando:

**Nicola BALZANO**

Anno Accademico 2023/2024

# Indice

[Tesi di laurea 1](#_Toc525114694)

[Una Base di Conoscenza di Supporto allo Sviluppo Software Orientato alla Privacy 1](#_Toc525114695)

[Indice 2](#_Toc525114696)

[1. Capitolo I 4](#_Toc525114697)

[Introduzione 4](#_Toc525114698)

[1.1 Privacy 5](#_Toc525114699)

[1.2 GDPR (General Data Protection Regulation) 7](#_Toc525114700)

[1.3 Privacy Oriented Software Development (POSD) 11](#_Toc525114701)

[1.3.1 POSD: Analysis 13](#_Toc525114702)

[1.3.2 POSD: Design 24](#_Toc525114703)

[1.3.3 POSD: Coding 30](#_Toc525114704)

[1.3.4 POSD: Verification & Validation 33](#_Toc525114705)

[1.3.5 POSD: Deploy 37](#_Toc525114706)

[2. Capitolo II 38](#_Toc525114707)

[Nuova Privacy Knowledge Base 38](#_Toc525114708)

[2.1 Privacy Design Pattern 39](#_Toc525114709)

[2.1.1 Pattern di Minimizzazione 39](#_Toc525114710)

[2.1.2 Pattern di Occultamento 43](#_Toc525114711)

[2.1.3 Pattern di Aggregazione 49](#_Toc525114712)

[2.1.4 Pattern di Informazione 52](#_Toc525114713)

[2.1.5 Pattern di Controllo 57](#_Toc525114714)

[2.1.6 Pattern di Rafforzamento 71](#_Toc525114715)

[2.1.7 Pattern di Dimostrazione 78](#_Toc525114716)

[2.2 Categorizzazione su Livelli dei Privacy Design Pattern 85](#_Toc525114717)

[2.2.1 Pattern Concettuali 86](#_Toc525114718)

[2.2.2 Pattern a Livello di Presentazione 88](#_Toc525114719)

[2.2.3 Pattern a Livello di Logica/Business 89](#_Toc525114720)

[2.2.4 Pattern a Livello di Dati 90](#_Toc525114721)

[2.2.5 Pattern a Livello di Architettura 90](#_Toc525114722)

[2.3 Diagrammi di Flusso delle Software Secure Architectures 91](#_Toc525114723)

[2.3.1 Diagrammi di Flusso SSA con Strategia orientata ai Dati 92](#_Toc525114724)

[2.3.2 Diagrammi di Flusso SSA con Strategia orientata ai Processi 103](#_Toc525114725)

[3. Capitolo III 113](#_Toc525114726)

[3.1 Privacy Knowledge Base Engine 114](#_Toc525114727)

[3.2 Specifica dei Requisiti 117](#_Toc525114728)

[3.2.1 Requi.siti Funzionali 117](#_Toc525114729)

[3.2.2 Requisiti Informativi 118](#_Toc525114730)

[3.2.3 Requisiti di Interfaccia 122](#_Toc525114731)

[3.3 Architettura del Sistema 126](#_Toc525114732)

[3.3.1 Struttura delle Classi 127](#_Toc525114733)

[3.3.2 Diagrammi di Sequenza 145](#_Toc525114734)

[3.3.3 Sistema Finale 148](#_Toc525114735)

[4. Capitolo IV: Conclusioni e Sviluppi Futuri 150](#_Toc525114736)

[5. Indice delle Tabelle 152](#_Toc525114737)

[6. Indice delle Figure 153](#_Toc525114738)

[7. Bibliografia 156](#_Toc525114739)

# Capitolo I

Introduzione

Al giorno d’oggi, l’utilizzo della tecnologia è diventato parte integrante della vita quotidiana, basti pensare ai *Social Network*. In Italia sono 34 Milioni gli utenti attivi (circa il 57% della popolazione) mentre nel mondo sono 3,3 Miliardi.

## Privacy

Il concetto.

## GDPR (General Data Protection Regulation)

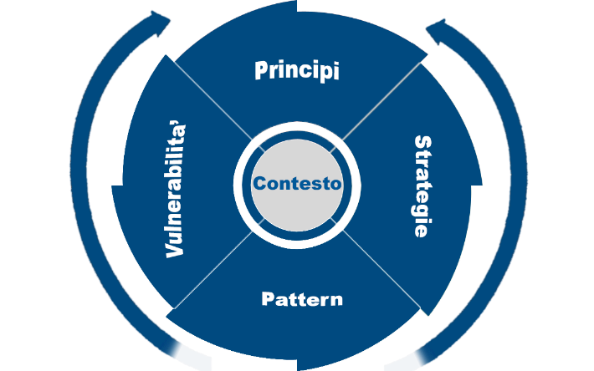


Figura 1 Privacy Knowledge Base del POSD

### POSD: Analysis

# Capitolo II

Nuova Privacy Knowledge Base

## Privacy Design Pattern

Privacy Design Pattern

# Bibliografia

[1] The Right to Privacy - Samuel D. Warren, Louis D. Brandeis *– Harvard Law Review, Vol. 4, No. 5 (Dec. 15, 1890), pp. 193-220*

[2] The Facebook-Cambridge Analytica Meltdown: Why GDPR is the Solution (blog.loginradius.com/2018/03/facebook-cambridge-analytica-meltdown-gdpr-solution/)

[3] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

[4] The 7 Foundational Principles, Implementation and Mapping of Fair Information Practices – Cavoukian A.

[5] Privacy Oriented Software Development – Antonio Maiorano – Università degli Studi di Bari “Aldo Moro“ (2017)

[6] Privacy and Data Protection by Design – from policy to engineering European Union Agency for Network and Information Security (ENISA)

[7] UC Berkley School of Information – Privacy Pattern. [Online] Disponibile a: <https://privacypatterns.org/patterns/>.

[8] Handbook of Privacy and Privacy-Enhancing Technologies. (The Case of Intelligent Software Agents) Van Blarkom, G.W.; Borking, J.J.; Olk, J.G.E. (2003).

[9]Tecnologie dell’informazione e della comunicazione -https://it.wikipedia.org/wiki/Tecnologie\_dell%27informazione\_e\_della\_comunicazione

[10] Agenzia per l’Italia Digitale (AGID) (2017) – Linee Guida per la modellazione delle minacce e individuazioni delle azioni di mitigazione.

[11] Guide to the Project Management Body of Knowledge (PMBOK® Guide)-Fourth Edition"

[12] HPE Security (2016) – Fortify Static Code Analyzer

[13]Open Web Application Security Project (OWASP) -https://www.owasp.org/index.php/Main\_Page

[14] OWASP – Top 10 2017 (2017), The Ten Most Critical Web Application Security Risks.

[15] OWASP (2014) – Top 10 Mobile Risk

[16] Agenzia per l’Italia Digitale (AGID) (2014) - Linee guida per lo sviluppo del software, Linee Guida per la configurazione per adeguare la sicurezza del software di base.

[17] Towards Organizational Privacy Patterns - Jan Porekar, Aljoša Jerman-Blažič, Tomaž Klobučar

[18] The Public Privacy – Patterns for Filtering Personal Information in Collaborative Systems - Till Schümmer

[19] A collection of Privacy Design Patterns - Munawar Hafiz

[20] The ABC of ABC: An Analysis of Attribute-Based Credentials in the light of data protection, privacy and identity - Merel Koning - Paulan Korenhof - Gergely Alpàr - Jaap-Henk Hoepman

[21] ABC4Trust EU Project - Official Website- <https://abc4trust.eu/index.php/home/fact-sheet>

[22] k-Anonymity: A model for protecting privacy - Latanya Seweney

[23] <https://en.wikipedia.org/wiki/K-anonymity>

[24] Development and Evaluation of Emerging Design Patterns for Ubiquitous Computing - Eric S. Chung, Jason I. Hong, James Lin, Madhu K. Prabaker, James A. Landay, Alan L. Liu

[25] Rethinking Privacy: Fair Information Practices Reinterpreted: <https://blogs.intel.com/policy/files/2015/01/RethinkingPrivacy.pdf>

[26] Collaborative Privacy Management System - In Joo Jang, Wenbo Shi, Hyeong Seon Yoo

[27] An Adaptive Privacy Management System for Data Repositories -Marco Casassa Mont, Siani Pearson, Pete Bramhall

[28] How to integrate legal requirements into a Requirements engineering

methodology for the development of security and privacy patterns

[29] Privacy Pattern Catalog - <http://privacypatterns.wu.ac.at:8080/catalog>

[30] Oracle Java Standard Edition 1.7 <http://www.oracle.com/technetwork/java/javase/overview/index.html>

[31] Oracle JavaFx SDK -<http://www.oracle.com/technetwork/java/javafx/install-javafx-sdk-1-2-139156.html>

[32] Drools Business Rule Management System - <https://www.drools.org>

[33] JavaFx Scene Builder - <https://www.oracle.com/technetwork/java/javase/downloads/sb2download-2177776.html>

[34] John Wiley & Sons - Pattern-Oriented Software Architecture, A System off Patterns, Volume 1