DESIGN PRINCIPLES - PRIVACY, QUALITY, AND SECURITY

After reading this factsheet you should:

- Have a basic knowledge of design principles around privacy, quality, and security.
- Understand who manages these design principles in the EU and US.

Who deals with design principles around privacy, quality, and security in the EU?

The design principles surrounding privacy, quality, and security are governed by several organisations and laws in the European Union (EU).

- General Data Protection Regulation (GDPR): Establishes Principles of Data Protection for the protection of personal data, how it is gathered, used, and stored.
- The European Data Protection Board (EDPB): Ensures that data protection rules are consistently applied across the EU.
- European Cybersecurity Act: Creates a framework for EU-wide cybersecurity certification and monitoring and is implemented by the European Union Agency for Cybersecurity.
- Network and Information Security (NIS) Directive: EU-wide regulations with a focus on strengthening the resilience and cybersecurity of vital infrastructure sectors.
- European Standardisation Organizations: CEN, CENELEC and ETSI are three European Standardisation Organization recognised by the European Free Trade Association (EFTA) as dedicated to creating and defining voluntary standards at the European level.

Who deals with design principles around privacy, quality, and security in the US?

The design principles surrounding privacy, quality, and security are governed by several organisations and laws in the United States (US).

- Federal Trade Commission (FTC): Implements several privacy and data security rules and regulations, including the Health Breach Notification Rule and Data Security.
- National Institute of Standards and Technology (NIST): Publications such as the NIST Privacy Framework and the NIST Cybersecurity Framework offer instructions on improving security and privacy practises.
- Health Insurance Portability and Accountability Act (HIPAA): creates standards for the privacy and security of protected health information (PHI).
- General Data Protection Regulation (GDPR): Impact on American companies that handle the personal data of EU citizens. Read more here.
- Payment Card Industry Data Security Standard (PCI DSS): A collection of security guidelines created by major credit card firms to safeguard cardholder data.
- General Data Protection Regulation (GDPR): Impact on American companies that handle the personal data of EU citizens.

What are the design principles around privacy?

To safeguard user information and foster trust, it is essential to design with privacy in mind. The following are some privacy-related design principles:

1. Privacy by Design: Privacy should be considered at the beginning of the design phase. Read more here.
2. Data minimisation: Gather and hold the minimum amount of personal information required to achieve the desired results. Only retain the data for as long as it takes to accomplish the result.
3. Consent: Before obtaining and utilising a user's personal information, obtain their informed and express consent. Read more here.
4. Transparency and User Awareness: The collection, usage, storage, and sharing of users' personal data should be transparently explained. Read more here.
5. Security and Data Protection.

What are the design principles around quality?

Designing with a quality focus guarantees that goods and services meet or surpass consumer expectations. The following are some quality-related design principles:

1. Quality by Design: Emphasis is placed on incorporating quality considerations into the design and development of goods, systems, and processes at the beginning of the design phase.
2. User- Centric Design: Create services and experiences that satisfy user needs maintaining them at the centre of your design process. There are several underlying principles of user- centred design.
3. Simplicity and Ease of Use: Reduce the learning curve by making the product or service simple for users to understand and navigate. Read more here.
4. Consistency and Standards: To produce a seamless and recognisable experience, adhere to established design patterns and standards. There are several underlying principles of consistency and standards.
5. Reliability and Performance: Make sure the product or system delivers a desired functionality and performance levels consistently.
6. Continuous Testing and Improvement: To find and fix any problems, conduct usability testing, functional testing, and performance testing. Read more here.

What are the design principles around security?

To safeguard systems, data, and users from unauthorised access, breaches, and threats, security must be a top priority during design. The following are some security-related design principles:

1. Secure by Design: Security should be considered at the beginning of the design phase.
2. Defence in Depth: Leverage multiple security measures to offer overlapping protections.
3. Secure Defaults: Make secure configurations and settings the default for systems, applications, and devices.
4. Principle of Least Privilege: Limit access to key resources and functions to help mitigate the effects of a security breach.
5. Secure Communication and Authentication: Implement robust encryption techniques, such as multi-factor authentication, to secure communication channels and safeguard sensitive data while it is being transmitted.

Health Innovation Hub Ireland
info@hih.ie
www.hih.ie

HIHI (UCC)
Western Gateway Building
University College Cork
Cork, Ireland
+353 (0)21 420 5560

HIHI (TCD)
H&H Building
St James' Hospital
Dublin 8, Ireland
+353 (0)1 896 2573

HIHI (University of Galway)
Lambe Institute
National University of Ireland
Galway, Ireland
+353 (0)91 492 072

HIHI (MTU)
CREATE Building
Munster Technological University
Cork, Ireland
+353 (0)21 432 6758