tsaaro
academy

EXCLUSIVE TSAARO ACADEMY NOTES GIVEAWAY

academy.tsaaro.com

About Tsaaro Academy

"It's not easy to build trust and manage risks at the same time"

Just getting a certification won't minimise nor guarantee your business from potential threats. It requires constant efforts and maintenance in securing the system from threats.

We at Tsaaro Academy provide the right training as per the international market standards to help data privacy professionals get access to the right skills to support their organisation with data privacy risks.

Our Official Partners

iapp OFFICIAL TRAINING PARTNER

PECB

DSCI PROMOTING DATA PROTECTION

EC-Council

qualityaustria central asia Succeed with Quality

Featured in

EXPRESS COMPUTER

CXO OUTLOOK Insights. Ideas. Inspirations

THE HINDU

All rights reserved by Tsaaro Academy

I. Three categories of IT Professionals

1. IT Developers

They are responsible for researching, designing, developing, and testing IT systems. Privacy concerns are less expensive to address in the early stages of development than during the later stages.

2. IT Acquisition

They help acquire open source or commercial software and hardware for the business needs of the organization. They are responsible for reviewing contracts to ensure that the necessary privacy requirements are included in the system targeted for acquisition.

3. IT Administration

Personnel is responsible for installing, configuring, and maintaining IT systems. The administrator is required to integrate technology into the organization‟s infrastructure and command the technical details of various technologies.

II. What is Privacy?

A privacy expert is prepared to distinguish different definitions of privacy and recognize when another person is using a particular definition to review and analyze an IT system. A few prominent viewpoints on privacy are:

1. Alan Westin’s Four States of Privacy characterizes an individual‟s expectation of privacy are:

a. Solitude: being free from others‟ observation.
b. Intimacy: individuals are a part of units that negotiate the rules of secrecy among themselves
c. Anonymity: freedom from identification and surveillance
d. Reserve: ability to withhold communication

2. Helen Nissenbaum’s Contextual Integrity: Privacy can be expressed as norms that should govern information access. Norms are domain-specific and context-specific which means that reasons for controlling access to one's information can differ based on individual expectations. This challenges IT professionals with the task of identifying relevant norms.

3. Daniel Solove's Taxonomy of Privacy: Activities and mechanisms that violate privacy such as interrogation and surveillance to compel information disclosure can help understand what privacy means. These activities can be used to determine when IT enables privacy-threatening outcomes.

4. Ryan Calo's Harm Dimensions: Objective harms are measurable and observable while subjective harms are not. But both their effect is similar on individual privacy because the individual takes similar steps to protect themselves. The challenge is to recognize the perception of harm. For this, IT professionals may rely on privacy notices and controls to build and retain trust.

III. What are privacy risks?

Privacy risks concern the likelihood that a privacy threat will exploit an IT vulnerability and the impact of this exploit on the individual and organization that retains information on the individual. The source of a threat/ threat agent could be;

1. Insider threat: e.g., employee personal information about a customer to later use that information to conduct fraudulent transactions on that person‟s behalf, called identity theft.

Nonmalicious insider threats can be due to carelessness, mistakes, insufficient training, weak security policies, and ineffective controls. (e.g., unencrypted backup drives and tapes that are stored in offsite locations that may be less secure than the primary work location).

2. External threat: These techniques include phishing, which is a form of social engineering that uses a routine, trusted communication channel to capture sensitive information from an unsuspecting employee.

Phishing is called spear-phishing or whaling when the activity targets high-profile personnel, such as corporate executives or HR managers who have more extensive access or access to more sensitive information.

IV. Privacy, security, and data

1. Privacy is commonly situated in the legal department of an organization; this requires frequent and efficient communication between the IT and Legal departments.The focus on privacy has often followed compliance with laws and regulations, which generally hold a narrower view of how privacy impacts individuals.

2. Security is traditionally defined as a set of activities that supports three different quality attributes: confidentiality, which ensures that information is only accessible by authorized individuals; integrity, which ensures that information has not been unintentionally modified; and availability, which ensures that information is readily available whenever it is needed.

While privacy certainly includes an individual"s ability to grant and deny access to their information, privacy also concerns an individual"s ability to control the granularity of information that others have access to.

3. U.S. regulations and international standards (Sarbanes-Oxley, Basel II, HIPAA)

have led to the development of data governance groups within organizations. These rules affect data management practices, and thus organizations respond by developing internal data governance policies to comply. Data governance policies are implemented by IT managers and leverage many of these same practices in the pursuit of improved privacy, such as identifying data assets and mapping regulatory controls onto IT systems that store governed data.

V. Privacy Principles and Standards

Privacy principles have their origin in the Fair Information Practices (FIPs), which were first established by the Health, Education, and Welfare Advisory Committee on Automated Data Systems in 1972. Other prominent principles include:

The Fair Information Practice Principles (FIPPs) (1977), published by the U.S. Federal Trade Commission (FTC), and The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), published by the Organization for Economic Cooperation and Development (OECD), etc.

The OECD guidelines state the following privacy principles:

1. Collection Limitation: there should be limits to the collection of personal data.
2. Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used.
3. Purpose Specification: purposes for which personal data are collected should be specified not later than at the time of data collection.
4. Use Limitation: Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified, except: (a) with the consent of the data subject; or (b) by the authority of law

5. Security Safeguards: Personal data should be protected by reasonable security safeguards against such risks.
6. Openness Principles: There should be a general policy of openness about developments, practices, and policies with respect to personal data.
7. Individual Participation: individuals shall have the right to obtain information from a data controller, and communicate regarding the use of information.
8. Accountability: data controller should be accountable for complying with measures that give effect to the principles stated above

VI. The Data Life Cycle

In the data life cycle, it is the responsibility of a privacy-respecting organization to specify the purpose for which information will be used and maintain consistency between actual uses and stated uses. The challenge for IT professionals is that the users of the data determine the purposes, and these purposes will evolve as the organization evolves its business practices. Data collection occurs at various points within an information system. A few types of data collection include:

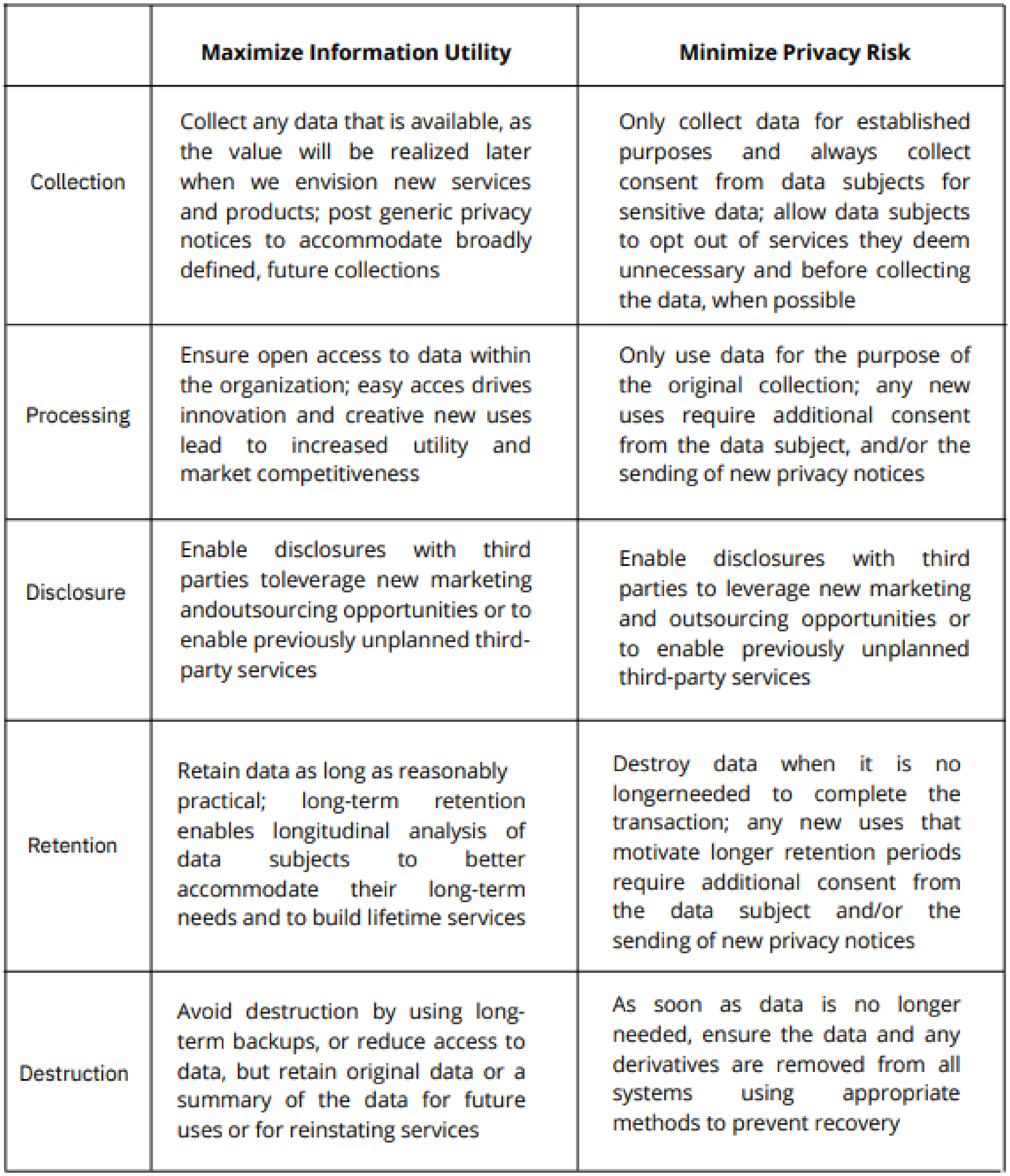
1. **First-party collection**, when the data subject provides data about themselves directly to the collector, e.g., in a web-based form that is only submitted when the data subject clicks a button;

2. **Surveillance**, when the collector observes data streams produced by the data subject without interfering with the subject‟s normal behavior;

3. **Repurposing**, which occurs when the previously collected data is now assigned to be used for a different purpose, e.g., reusing a customer‟s shipping address for marketing and

4. **Third-party collection**, when previously collected, information is transferred to a third party to enable a new data collection.

The data life cycle is shaped by the privacy objectives and business practices of an organization and the systems that they develop will be adapted to meet these objectives. Data the life cycle from two extreme perspectives: 1. a maximize-information-utility objective, which views data as the basis for monetization and new revenue and seeks to collect and retain as much data as possible and; 2. a minimize-privacy-risk objective, which views data as potentially toxic with inherent risks that can result in significant, irreversible privacy harms.



	Maximize Information Utility	Minimize Privacy Risk
Collection	Collect any data that is available, as the value will be realized later when we envision new services and products; post generic privacy notices to accommodate broadly defined, future collections	Only collect data for established purposes and always collect consent from data subjects for sensitive data; allow data subjects to opt out of services they deem unnecessary and before collecting the data, when possible
Processing	Ensure open access to data within the organization; easy acces drives innovation and creative new uses lead to increased utility and market competitiveness	Only use data for the purpose of the original collection; any new uses require additional consent from the data subject, and/or the sending of new privacy notices
Disclosure	Enable disclosures with third parties toleverage new marketing andoutsourcing opportunities or to enable previously unplanned third-party services	Enable disclosures with third parties to leverage new marketing and outsourcing opportunities or to enable previously unplanned third-party services
Retention	Retain data as long as reasonably practical; long-term retention enables longitudinal analysis of data subjects to better accommodate their long-term needs and to build lifetime services	Destroy data when it is no longerneeded to complete the transaction; any new uses that motivate longer retention periods require additional consent from the data subject and/or the sending of new privacy notices
Destruction	Avoid destruction by using long-term backups, or reduce access to data, but retain original data or a summary of the data for future uses or for reinstating services	As soon as data is no longer needed, ensure the data and any derivatives are removed from all systems using appropriate methods to prevent recovery

KICK START YOUR CAREER

Enquire For Training at Tsaaro Academy

info.academy@tsaaro.com
+91 93353 36454