CONTENT ETHICS – DATA PRIVACY

INTRODUCTION

Data privacy has been a central ethical issue since the introduction of mainframe computers in the 1970s. Now, in the 2020s, it has been codified into law in numerous nations. In the European Union, the GDPR applies in member nations but also has broader reach in its influence on other countries legislation. In the United States, sectoral laws and regulations have been in place for a number of years (e.g., HIPAA), while comprehensive laws have recently passed in some states (e.g., California CCPA, Virginia CDPA). (See acronym table at end.) All 50 US states have some form of data breach law. Any ecm implementation that manages personal information (PI), which is likely to be most of them, needs to address legitimate privacy expectations and comply with all applicable privacy laws (statutes, regulations, case law). Data privacy considerations should be incorporated into all stages of the software development and implementation lifecycle, as well as in system operations.

DEFINITION

The scope of data privacy. ". . .concerns the creation, use, access to, and dissemination of personal information or data, where "information" and "data" are understood to cover a broad range of formats and media types." (Ethics for Records and Information Management, pg. 119) Personal information (PI) is any . . . "data that is about a person, whether by directly identifying the person or by providing a basis of inference about the identity of the person. (Ibid.) In addition to PI, the acronyms PII (personal identifiable information) and PHI (personal health information) are used in various contexts and statutes (e.g., PHI in healthcare and HIPAA). Within the U.S. legal context, privacy restrictions have focused on the management of personal information and the harms attendant to mismanagement (such as improper disclosure, poor security, unjustified retention). In the EU legal context, the scope of privacy concerns is broader and concerns the processing of data and the protection of rights. (See *Determann's Field Guide to data Privacy Law*, 3rd, secs. 0.15-0.16) (New U.S. laws, however, have incorporated aspects of EU law, in particular, the GDPR, into their provisions. The CCPA is an example.

Legal and ethical obligations implicated by digital content can be divided (roughly) between the **ethical management of data** and the **management of ethical and legal rights**. The **scope of data management** includes **capture, access, disclosure and retention**. The **scope of rights management** includes managing **data subject requests (DSARs)** and **consent / preference management**. DSARs can include requests for records of the data subject's PI, requests for copies, and even requests for erasure (right to be forgotten).

Ecm technologies provide means and methods for addressing data and rights management obligations. They should be designed at the development and implementation stages, and deployed at the operational stage to do so. Complying with legal requirements and reasonable expectations (customers, constituents, employees) presents challenges, but failure to address data privacy within the context of a **digital transformation** initiative will be a missed opportunity at best, negligence at worst.

AN ECM DATA PRIVACY ROADMAP

In charting your data privacy course, a number of **frameworks** provide guidance for the **design of ecm** and other solutions. There are numerous **fair information privacy practices** frameworks (**FIPPs**). Canada and the U.S. both have FIPPs. The **OECD privacy principles** have guided EU legislation. The **Generally Accepted Privacy Principles** (**GAPP**) from the **American Institute of Certified Public Accounts (IACPA)** and **Canadian Institute of Chartered Accountants** (**CICA**) provides the best framework for organizing your data privacy strategy within an ecm digital transformation initiative. It is designed to support audits (which is not coincidental, given its provenance). The GAPP framework is also supported by a **maturity model** for implementing privacy programs. Some elements of the maturity model may be useful for defining requirements and measuring the success of a deployment. These principles provide a framework for both the management of personal information and the management of data subject rights.

The principles are listed below with descriptions of each. (For more information, see the CPA Canada site.)

1. Management.	The entity defines, documents, communicates and assigns accountability for its privacy policies and procedures.
2. Notice.	The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed.
3. Choice and consent.	The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use and disclosure of personal information.
4. Collection.	The entity collects personal information only for the purposes identified in the notice.
5. Use, retention and disposal.	The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulation and thereafter appropriately disposes of such information.
6. Access.	The entity provides individuals with access to their personal information for review and update.
7. Disclosure to third parties.	The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. Security for privacy.	The entity protects personal information against unauthorized access (both physical and logical).
9. Quality.	The entity maintains accurate, complete and relevant personal information for the purposes identified in the notice.
10. Monitoring and enforcement.	The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes

While some of the categories are administrative/organizational, most can be used to (a) **identify needs**, (b) **organize requirements** and (c) **group solution components**. In this sample below, one or two

requirements are mapped to each principle. In a real-world example, pages will be dedicated to requirement areas.

1. Management.	System Requirements
2. Notice.	▪ Noticing information or links to notice appear on PI data gathering digital forms.
3. Choice and consent.	▪ Consent record captured and status set to effective. Updated / replaced when new consent preferences are captured. ▪ Requirement: Consent record linked to in-scope PI.
4. Collection.	▪ Ingestion restricted to document / content types specified in data capture policy. ▪ Fields / metadata support PI management requirements (e.g., DSAR retrieval, security).
5. Use, retention and disposal.	▪ Workflows / case management flows are configured for original business purposes. Consent check is built in as a processing condition. ▪ New workflows have consent check for additional authorization. ▪ Retention is automated based on document date or event.
6. Access.	▪ The user access model follows the minimum necessary rule. o Users are restricted to documents based on role + legitimate purpose. o Access restriction is at the record / content type level or sublevel (e.g., metadata value).
7. Disclosure to third parties.	▪ A mechanism exists to check authorization prior to disclosure to third party (outside user access model). Minimally, authorization is detectable as part of the search or workflow. Ideally, disclosure is blocked if authorization is not detected.
8. Security for privacy.	▪ Content and data encrypted (at rest). ▪ Servers use TLS for communication. ▪ Data sources (file share, databases) use encrypted access methods.
9. Quality.	▪ Capture processes provide quality control steps where appropriate. ▪ Index data validated against system of record. ▪ Records not alterable without authorization (trusted systems standards met)
10. Monitoring and enforcement.	▪ Audit trail created for all activities on documents / content. Edits, views, etc and linked to user.

CONCLUDING THOUGHTS

Using the GAPP principles or other FIPPs as a road map for defining, building and implementing privacy requirements realizes a **privacy-by-design (PbD)** approach, which is a requirement of the GDPR. PbD treats data privacy as a core feature set of solutions, not just a constraint. (See my article on the topic of **ECM and Privacy by Design** for a full explanation.) Further, because GAPP and the other FIPPs have served as starting points for legislation and regulation drafting, they can be used to create a **generalized solution model** that applies across jurisdictions and that can be further specified to address the details of a given law. This will be important to organizations within the jurisdiction of multiple laws. It will be

especially helpful to developers and implementers who create solutions for customers in multiple sectors and geographies.

ACRONYMS

Below is a table of acronyms used in this article.

CCPA	California Consumer Privacy Act
CDPA	Virginia Consumer Data Protection Act
DSAR	Data Subject Access Request
FIPP or FIP	Fair Information Privacy Practices or Fair Information Practices
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
OECD	Organisation for Economic Cooperation and Development
PHI	Personal Health Information
PI	Personal Information
PII	Personal Identifiable Information