Effective Data Protection Governance Project: Improving Operational Efficiency and Regulatory Certainty in a Digital Age[1]

Executive Overview[2]

July 2016

[1] The Information Accountability Foundation (IAF) was founded in 2013 to conduct research and further education on accountability based governance. The IAF has its roots in the Global Accountability Dialogue that defined the essential elements of accountability in 2009. The IAF created the Effective Data Protection Governance (EDPG) Project in 2015 to give focus to the full range of issues related to the legal, fair and just processing of information given the growing complexity of information ecosystems.

[2] For a full EDPG overview, see http://informationaccountability.org/wp-content/uploads/Effective-Data-Protection-Governance.pdf.

The Effective Data Protection Governance Project

The accelerating evolution of information and communication technologies changes the power equilibrium between people, government and organisations in unpredictable ways. This shift in power suggests a need to re-think what obligation(s) are appropriate with respect to the collection and use of data about an individual, when and how an individual should participate, and how data and its use is governed.

Privacy and data protection law and the business practices associated with the processing of data in a legal, fair and just manner are undergoing revision to catch up with these massive changes taking place in technology. The European Union's General Data Protection Regulation ("GDPR") is just the first wave of those modifications. Changes will be seen in Latin America, Canada, Asia, the United States and Africa. Some changes will be explicit revisions of laws, while other changes will use the flexibility built into laws, such as codes of conduct, to better align the interests of all stakeholders.

These changes do not mean the abandonment of key societal values captured by privacy and data protection law. Instead, they reinforce the need for fair processing that enables data to create knowledge-based value. The development and implementation of evolving governance concepts requires a full, 360-degree view of the dynamics in play, with a heavy emphasis on the impact to individuals. Information policy cannot be dependent on a single approach.

Today's information dependent economy, for example an "IoT" ecosystem, highlights the complexity of the world we live in. The many participants, the scope of all the data flows, the myriad of data uses and the rapid growth trajectory of this information ecosystem are all challenging our current approach to data governance. Individuals and organisations in the ecosystem have complex data exchange relationships with each other. Some of these relationships are direct and exist between the individual and a business, and other relationships are indirect and are not initiated by the individual.

To add to the complexity, all data, not just personally identifiable data, can have an impact on an individual, and new uses and new exchanges of data can trigger questions on the "sensitivity" of the data, even if by classification the data itself was not originally sensitive. At the same time, if sensitive data is used for operational reasons, such as securing the ecosystem, then different and even fewer obligations by a participant should apply.

Developing a governance model for such an information dependent ecosystem, such as an IoT system, one that assures fairness, protection and innovation, and components that can be implemented as needed, is the objective of the EDPG Project. The project is based on a vision that data should be used to drive innovation in complex data ecosystems creating value for all stakeholders while protecting individuals and individuality.

The EDPG Project has identified four areas where improvement in governance is needed. First, all the participants in the ecosystem must be held accountable for new obligations. Second, the factors related to the data coupled with the data use must be considered together with added consideration of the sensitivity of the data, the sensitivity of the use, as well as the identifiability of the data. Third, the complexity of this environment does not allow for straightforward guidance. Instead a comprehensive data impact assessment (CDIA) must be conducted which

determines what is appropriate collection and use of the data and how risks, especially risks to the individual, can be mitigated.

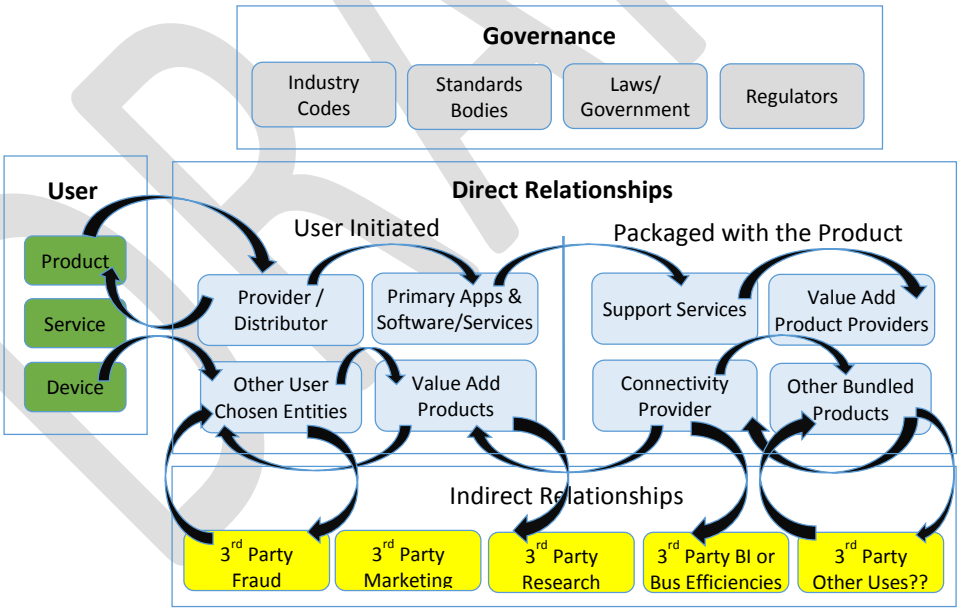
Fourth, as more and more data is being passively collected, created and used, often without the knowledge or involvement of the individual, the obligations for each participant, particularly those related to how and when individuals are engaged, must be rethought.

The EDPG approach places more of the responsibility for assuring fairness to business participants, engaging with the individual when there is an appropriate and meaningful need for them to have some choice over data about them that is collected and used.

The EDPG Project Proposes Improvements in All These Governance Areas

- **Ecosystem Participants[3]:** The complexity of evolving information ecosystems is exploding. There are too many players for the individual to ever understand all aspects of how data is collected, used and shared. More and more data exchange is taking place, making it too much for one participant, especially the individual (user), to provide effective governance across the whole ecosystem.

Chart 1. Ecosystem Participants & Relationships



Data is either collected and used from a user or device and is actively or passively shared with a number of direct participants in the ecosystem. But data is also increasingly coming from sensors or is "created" as a result of an analytical process. Participants may have arrangements with other indirect participants who provide ancillary services to the primary participants and may not be known to the user or device. Also, data may be shared with

[3] Participants are generally "business" organisations. While individuals do participate in information ecosystems, they should not and cannot play a dominant role in the governance of information.

third parties in either personally identifiable or de-identified form. Finally, there are governance participants such as regulators or self-regulatory entities who have a say in what data is collected and used for what purpose.

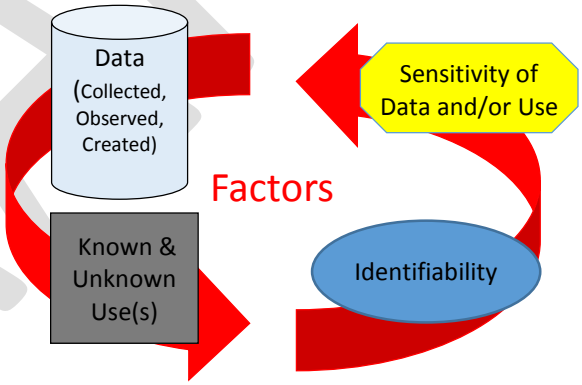
Each participant, whether directly known to the individual or not, must be accountable for their respective obligations based on the data they collect or receive, how they use the data, and with whom they share the data.

- **Factors:** There are four factors that each participant must consider in combination to provide effective data governance.

  The first two are the data itself coupled with the intended use(s) of the data by the participant. In addition, the sensitivity of the data and the sensitivity of the use must be considered. Finally, the identifiability of the data (whether it is personally identifiable, pseudonymous or de-identified in some way) must also be considered.

  It is the intersection of the data, the intended use(s), the sensitivity and the identifiability that in combination dictate what obligations are appropriate for each participant. All these factors interrelate in assuring effective data governance.

Chart 2. Key Factors for Data



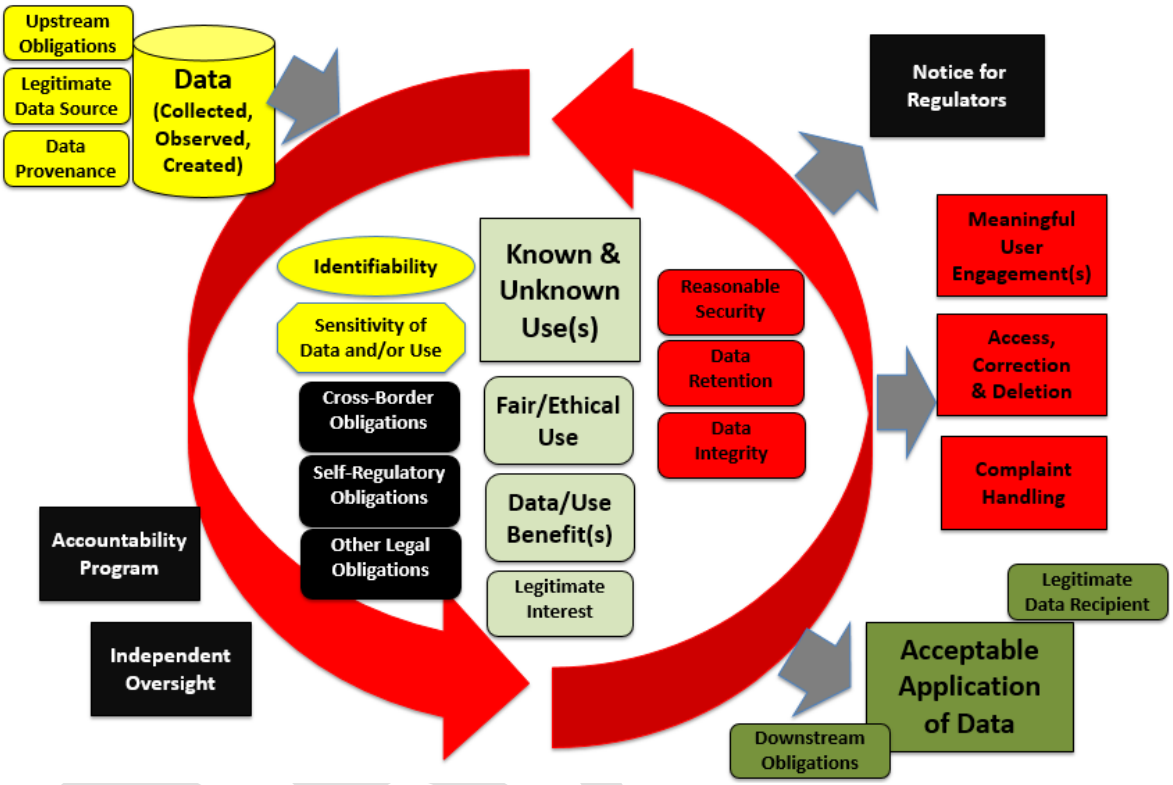
- **Risk Assessment:** As the myriad of data and uses expands, it is impossible to predetermine what is an acceptable or an unacceptable application of the data. Thus, each participant in the ecosystem must conduct a CDIA that includes ethical implications and the impact to the individual to determine what is an appropriate use of data and what is not. Privacy Impact Assessments (PIAs) have been the traditional approach, but the EDPG framework recommends these be expanded to consider more factors, particularly for projects/products that are data intensive.

  Businesses may conduct CDIA's[4] based on guidance from industry codes or other similar approaches acceptable to the jurisdiction that identifies the appropriate obligations for each business participant. The obligations will likely vary for each participant based on their role in the ecosystem.

  While businesses will have the freedom to conduct CDIAs to determine when and how best to engage individuals, this is not the only purpose of CDIAs. Businesses will have to demonstrate to regulators/DPAs, if asked, that the uses of data are not only legal but also fair to the individual.

[4] A full CDIA is contemplated for a scenario that is data intensive. A scaled down version would be used for a less data intensive scenario that encompasses the goals of a PIA.

Chart 3. Framework for Ethical Data Governance: Comprehensive Data Impact Assessment



- **Obligations:** As more and more data is being passively collected, created, used and shared across increasingly complex ecosystems, often without the knowledge or involvement of the individual, the obligations expected of each participant needs to be rethought, placing more of the responsibility for assuring fair processing of the data to the business participant, engaging with the individual only when appropriate and where meaningful choice is relevant.

  The EDPG approach proposes a new way to think about achieving the needed levels of transparency and participation by the user. There are several components.

  First is a new way to think about transparency. The EDPG approach recommends that companies post a comprehensive privacy notice written for regulators/DPAs. These longer notices will cover its policies and practices relating to information collection and use as well as information governance (including its CDIA process)[5]. While these notices are available to Individuals, they are not required, or expected, to read or acknowledge them.

[5] Content parameters of this detailed type of notice are still in development. It is anticipated the overview of an organisation's governance would be high-level with more information available to a regulator/DPA upon request.

Next, the EDPG approach engages individuals in data collection and data use issues only where they can participate in an easy and meaningful way. Securing the ecosystem, operating the product or preventing fraud are examples of data use where individual control or choice over the use of data is not common, and active engagement with the individual adds little to effective governance. These uses of data, however, should carry obligations, such as appropriate security, that should be addressed in the longer notice. However, these uses do not have to be part of a meaningful individual engagement obligation. At the same time, there are uses (including collection) of data where an individual should be engaged and provided meaningful control over the data about them.

The EDPG Project Benefits Individuals, Regulators/DPAs and Businesses

The EDPG approach does not rely on notices to inform individuals, and it does not expect individuals to govern collection and use of data about them through unread and unreadable notices. Instead, the approach involves the whole ecosystem, focuses on what the data is and how it is used, includes a robust risk assessment, and provides individuals with more meaningful and flexible engagement where individual control is effective while putting stronger obligations on the business participant to protect the individual. The approach:

- Provides a more thorough application of data protection to all data that includes what is currently non-personal data that is not covered by most data protection laws. In addition, it provides more effective information governance covering a broader range of interests.

- Creates more accountability for business participants and thus enforceability over responsible business use of data about individuals, including areas that are not subject to direct regulation, and/or where a direct individual relationship may not exist.

- Eases the burden on regulators/DPAs by providing more transparency about how businesses collect and process data through the comprehensive notice written by lawyers for regulators/DPAs.

- Includes a broader set of interests and risks that allows businesses to more aggressively leverage information to create value. Through codes of conduct or similar processes, organisations will have greater clarity about what is expected of them.

The EDPG Approach Can be implemented in Phases

It is envisioned that the EDPG approach would be implemented in stages. In different geographies, there could be a slightly different starting point that is compatible with local law, but is still consistent with the overall approach. The EDPG approach has the flexibility to make use of codes of conduct or other similar mechanisms, where appropriate.

The approach supports both long-term and short-term objectives. In its totality, the EDPG components satisfy the long-term governance needs of an information dependent ecosystem. In the short-term, the individual components can provide solutions for current regulatory challenges. For example, the adoption of the CDIA is an opportunity to look at supporting the

implementation of specific legal requirements in Europe. In other instances, like Canada, the EDPG approach will help inform the processes that create confidence in using implied consent. In other regions, the EDPG approach will help inform the debate on new legislation to create interoperability around concepts such as accountability, all to enable the effective governance of fair data processing.

Conclusion[6]

Under the EDPG approach, the obligations that fall on each business participant will be determined by the combination of the data itself and the use of the data, along with additional factors like the identifiability and the sensitivity of the data. In short, a more balanced, fluid and contextually flexible set of obligations can better achieve today's information governance objectives. Inherent in this overall approach are five (5) interconnected components:

1. **Ecosystem Complexity** – Effective data governance will be successful only if the approach requires ALL participants in an information ecosystem to accept their designated role and corresponding responsibilities and accountability obligations.
2. **Data and Data Use Factors** – The EDPG approach recognises that both data and data use with additive considerations of "identifiability" and "sensitivity" are key to both assessing risk to all stakeholders and to developing commensurate mitigations and determining relevant obligations. More inclusive analysis of all these factors by participants will be required.
3. **Comprehensive Data Impact Assessments** – To achieve an effective mitigation of risks and realise the benefits from the opportunities to use data, a new approach to "assessments" is required. The EDPG approach builds on the concepts of PIAs but takes the assessment to a more comprehensive level assessing all relevant interests of the business and the individual.
4. **Obligations and Accountability** – New, more complex information ecosystems mean new ways to determine and action established obligations and call for new ones. Business participants should have, in particular, meaningful, appropriate and innovative ways to engage with individuals to ensure they have suitable **participation** and a means to exercise control where relevant. Business participants will also shoulder stronger obligations to assure fair and balanced processing of data. This includes the ability to demonstrate a business participant's accountability, including internal oversight and monitoring.
5. **Enforcement** – In some jurisdictions, the shift in responsibility to business participants may mean different enforcement processes are needed to ensure data collection and use are legal, fair and just. While codes of conduct may be one way to enhance enforcement and ensure business "processes," such as CDIAs, are adequate, the EDPG approach recognises that regulators may need new tools to ensure effective enforcement.

[6] The IAF has been working internally on the EDPG Project since early 2015 and while parts of the EDPG Project are more advanced and are ready to socialise, test and refine with other stakeholders, other parts are less developed. Over the coming months, the IAF plans on further developing, testing and socialising this approach, including exploring how the entire framework or components may fit into or support the implementation of local laws.