# Compare Results

| Old File: | | New File: |
|---|---|---|
| **Item 2 Data Privacy Guidelines Implementation Plan - DRAFT.pdf** | versus | **Data Privacy Guidelines Implementation Plan - DRAFT final.pdf** |
| **11 pages (727 KB)** | | **11 pages (695 KB)** |
| 2/17/2022 12:17:45 PM | | 3/18/2022 8:28:22 AM |

**Total Changes**

**41**

Text only comparison

**Content**

17 Replacements

14 Insertions

10 Deletions

**Styling and Annotations**

0 Styling

0 Annotations

Go to First Change (page 1)

# Proposed Data Privacy Guidelines Implementation Plan – FINAL DRAFT

## Summary:

In March 2021, the Data Privacy Guidelines were passed to help the City of Long Beach (the City) and its partners incorporate privacy by design as we deploy new technologies and new services in Long Beach. The Data Privacy Guidelines Implementation Plan aims to operationalize these guidelines and provide the City with next steps on how to build public trust through excellence in data privacy, data security, and community engagement.  Policy recommendations are broken into 3 categories: capacity building, process, and education and communication recommendations.

| Data Privacy Policy Recommendations | |
|---|---|
| 1. | Hiring Data Privacy Staff |
| 2. | External Privacy Advisory Commission |
| 3. | Data Privacy Guidelines Implementation Workgroup |
| 4. | Surveillance Ordinance |
| 5. | Privacy Impact Assessments |
| 6. | Proposed Use Policies |
| 7. | Guidelines for Data Collection |
| 8. | Implement Data Privacy in the Procurement Process |
| 9. | Community Education Campaigns |
| 10. | Educating Staff on Data Privacy |
| 11. | Data Privacy Website |
| 12. | Implement Technology to Prevent Data Loss |

## Capacity Building Recommendations

### 1.  Hiring Data Privacy Staff

*Description*

Operationalizing the Data Privacy Guidelines will require dedicated staff who can create and support data privacy programs. While some recommendations may be able to be addressed by existing staff, significant policy changes will require additional staff.

The City of Portland's data privacy programs are led by one Program Coordinator. This Program Coordinator's main role is to create a data privacy toolkit and educate other department staff on data privacy.

The City of Seattle has a fully staffed data privacy office, including 3 Privacy Analysts, 1 Manager, and 1 Chief Privacy Officer. This allows them to have a more robust data privacy program. Their office acts as consultants and guides to other departments interested in utilizing a new technology. They also manage the City's data privacy programs.

The City of Oakland has a Commission liaison that supports the work of their Advisory Commission.

*Resources Required*

There are several different avenues that the City of Long Beach can take when staffing data privacy programs. Having one, dedicated FTE to data privacy can help the City create a data privacy program, process, and resources. As the data privacy program and process is built out, more staff may be needed to run the programs and process.

This will take a significant effort to dedicate funds to support full-time staff. TID Leadership will need to determine what data privacy initiatives they are interested in and how they want a staff member to support these initiatives.

*Guidelines Covered*

This recommendation has the potential to cover Data Privacy Guidelines 1, 2, 3, 4, and 5.

## 2. External Privacy Advisory Commission

*Description*

To gain public guidance and leadership on data privacy initiatives, an External Privacy Advisory Commission can be formed. An External Privacy Advisory Commission can be utilized to advise TID staff when creating a data privacy program. An Advisory Commission will allow us to leverage community expertise and will augment staff capacity.

In the City of Seattle, staff utilized a Privacy Advisory Committee of area data privacy thought leaders from academia, local companies, private legal practice, and community activist groups to provide best practices recommendations on their data privacy programs.

The City of Oakland utilizes a Privacy Advisory Commission to provide advice on best practices to protect residents' privacy rights in connection with the City of Oakland's purchase and use of surveillance equipment and other technology that collects or stores data. This Commission also approves Impact Assessments and Use Policies for the City of Oakland. The commission members are officially appointed by the Mayor.

*Resources Required*

TID staff will need to identify local community leaders from different industries, including technology, data, human rights, and other areas, who can serve on a Privacy Advisory Commission. This commission should be made to reflect the diverse community of Long Beach. There will also need to be support from TID staff to convene this group and present data privacy recommendations for their input and guidance. In other cities, a privacy analyst or program coordinator leads this effort. Furthermore, the commission will need administrative staff support.

*Level of Effort and Time Commitment*

This recommendation will require staff time to plan the commission's structure and what kinds of individuals should be on it as well as recruiting these individuals to serve on the commission. After its formation, the group will be consulted on an on-going basis for guidance on the City's data privacy programs.

*Guidelines Covered*

This recommendation covers Data Privacy Guidelines 2, 3, and 4.

## 3. Data Privacy Guidelines Implementation Workgroup

*Description*

Forming an internal Data Privacy Guidelines Implementation Workgroup can help to gain an organizational view of what data privacy measures the City may take. This group should consist of representatives from all Departments, especially those who have the most data privacy concerns. Involving representatives from all departments encourages a participatory process and can create ownership of the data privacy process throughout the organization. Involving input from other departments can also help TID staff gain an understanding of the feasibility of data privacy initiatives from an organizational standpoint. This group will also help implement data privacy and equity initiatives throughout the City.

TID staff will present data privacy work to this group and use their feedback to guide their work. This group will be able to provide perspective and validate data privacy work done by TID staff. The City of Portland has utilized a Data Privacy Implementation Workgroup to guide their data privacy efforts and implement data privacy programs throughout the organization. One Data Privacy Program Manger leads this Workgroup in Portland.

A workgroup can also evolve into a Data Privacy Champions group to continue to build capacity around data privacy. Similar to the Equity Champions in each Department, a data privacy champion would receive training about data privacy and would assist in furthering data privacy efforts in their Department. The City of Seattle has piloted this model to help implement data programs in the organization.

*Resources Required*

This will require facilitation of the workgroup by a TID staff member. There will also need to be organizational buy-in to coordinate representatives from each department. TID Staff will need to prepare presentations on work around data privacy and facilitate conversations around data privacy with the group. Furthermore, TID staff will be tasked with implementing suggestions offered by the workgroup.

*Level of Effort and Time Commitment*

Depending on the frequency that the workgroup meets, this will require staff time to host the meeting and work on initiatives. In other cities, like the City of Portland, one FTE is devoted to data privacy and leads the workgroup. Implementing a data privacy plan can take over a year. This workgroup could also build upon Data Policy Steering Committee (DPSC) and the Smart City Initiative Technical Advisory Committee.

*Guidelines Covered*

This recommendation covers Data Privacy Guidelines 3, 4, and 5.

## Process Recommendations

### 4. Surveillance Ordinance

*Description*

Passing an ordinance can help create a data privacy program with clear requirements on how the City should operate in protecting residents' data. Nearly all cities with data privacy programs and offices have a surveillance ordinance that they tie their work to. This ordinance can outline what steps the City must take to protect residents when gathering private information and employing new and existing technologies. These ordinances also create a process for analyzing new technologies and their potential privacy impacts. Many of these ordinances also call for the City to publish an annual state of privacy report.

The City of San Diego's Surveillance Ordinance, the Transparent and Responsible Use of Surveillance Technology (TRUST) ordinance, establishes processes for creating transparency, accountability, and public deliberation informing the City of San Diego's acquisition and usage of surveillance technology.

*Resources Required*

A surveillance ordinance will require the community's and City Council's support in drafting and passing it. Many cities have used the ACLU's Community Control Over Police Surveillance (CCOPS) Model Bill as a reference and guide when drafting their own legislation.

*Level of Effort and Time Commitment*

This will require a high level of effort from TID staff to assist in drafting the ordinance and briefing Council and management on its' effects. In other cities' this process can take about a year.

*Guidelines Covered*

This recommendation covers Data Privacy Guidelines 1, 2, 3, 4, and 5.

## 5. Privacy Impact Assessments

*Description*

Privacy Impact Assessments (PIA) identify the anticipated impact technologies employed by the City will have on privacy. A PIA asks questions about the collection, use, sharing, security, governance, and access controls for data that is gathered when using a technology or program. It also requests information about policies, training, and documentation that govern the use of the technology. PIAs can include questions that assess a technology's risk to racial equity.

The results of a PIA are used to determine privacy risks associated with a project and suggest mitigations that may reduce some or all of those risks. In cases where risk cannot be appropriately mitigated PIAs can disallow the technology altogether. PIAs should be posted to a public-facing website to promote transparency. PIAs are typically issued through a public process. The Department employing the technology will write the PIA, TID staff will review it, the PIA will be available for public comment, the Department and TID staff will make changes, then the PIA will be approved by the Council and posted to a public-facing City website.

Several organizations including the City of Oakland and Seattle and the County of Santa Clara publish Privacy Impact Assessments. These Assessments are created internally and posted on external-facing websites for transparency. In most cities and counties PIAs are reserved for surveillance technologies or projects that gather significant personal identifying information. Additionally, criteria about what technologies or programs should go through the PIA process are often outlined and tied to a surveillance ordinance. PIAs can be performed retroactively to identify privacy risks and offer mitigation recommendations for existing technologies. With new technologies, the PIA can accompany the contract approval of the technology but does not need to be approved before the City enters into an agreement with a vendor.

PIA's can be triggered by a surveillance ordinance or done on a case-by-case basis sparked by the interest of a Privacy Advisory Commission.

*Resources Required*

To implement this process City wide, there will need to be organizational and executive buy-in. This will require TID to create a process for completing PIAs, including creating a template, educating staff throughout the City on how to complete a PIA, then serving as a resource to review PIAs and analyze public comments. Staff should also determine how and if PIAs will be tied to City Council approval and/or reviewed by a Privacy Advisory Commission.

*Level of Effort and Time Commitment*

This will require effort from TID staff to create the PIA process. Once the process is created, TID staff will act as a facilitator of the process for Departments completing PIAs. This will add another layer of work when implementing new technology but has the benefit of identifying privacy and equity risks before technology or program causes harm. Establishing a PIA process can take about a year to do and is led by one FTE. After establishing the process, it can take departments around 1-3 months to complete a PIA.

*Guidelines Covered*

This recommendation covers Data Privacy Guidelines 1, 2, 3, 4, and 5.

## 6. Proposed Use Policies

*Description*

Proposed Use Policies create a transparent guideline for how technologies can be used. Use policies can outline the purpose, authorized use, data collection, data access, data protection, data retention, public access, third-party data-sharing, training, auditing and oversight, and maintenance of technologies used by the City. Proposed Use Policies should be posted to a public-facing City website. In the City of Oakland, Proposed Use Policies accompany PIAs and clearly outline the uses of certain technologies.

To implement this process Citywide there will need to be organizational and executive buy-in. This will require the Department that is implementing policy to assist in filling out the use policy and TID staff to review the use policy. Staff should also determine how Proposed Use Policies will be reviewed by the public or a Privacy Advisory Commission.

*Level of Effort and Time Commitment*

TID staff will need to create a proposed use policy template. Both external and TID staff time will be required to complete use policies for technologies. Use policies, can take about 1-3 months to be completed after the process is created.

*Guidelines Covered*

This recommendation covers Data Privacy Guidelines 1, 2, 3, 4, and 5.

## 7. Guidelines for Data Collection

*Description*

Guidelines for Data Collection provide recommendations to staff about how to collect data and protect the privacy of residents. Creating these Guidelines can inform staff about when to collect private data, best practices in collecting private data, and how to manage this data. These guidelines can encourage staff to limit their collection of personal information when distributing surveys or collecting data during public engagement events.

*Resources Required*

This recommendation requires TID Staff and stakeholders to create these guidelines. TID staff will also create a shareable document with guidelines of when to collect personal identifying information and recommendations for mitigating privacy risks. In other cities, there is typically 1 FTE leading this work as well as other data privacy projects.

*Level of Effort and Time Commitment*

This will require effort from TID staff to create the document and promotion of these guidelines to all departments. It can take around 3 months to develop this type of document. The document should be updated annually.

*Guidelines Covered*

This recommendation covers Data Privacy Guidelines 4 and 5.

## 8. Implement Data Privacy in the Procurement Process

*Description*

The Data Privacy Guidelines should be embedded into the work vendors and external partners do. This can be achieved by adding screening questions about data privacy and equity into vendor contracts, the Vendor Information Security Assessment (VISA) Questionnaire, and the City's Request for Proposal (RFP) Template.

*Resources Required*

This requires TID staff time to review these documents and insert screening questions that can help the City understand how the vendor will collect and manage sensitive data. Procurement staff will also need to review these questions and implement them into these forms.

*Level of Effort and Time Commitment*

Both TID and Procurement staff time will be required to implement screening questions into these forms. After this, staff must be trained on how to assess answers to these questions when reviewing RFPs.

## Education and Communication Recommendations

### 9. Community Education Campaigns

*Description*

Community Education Campaigns can serve as a tool to educate residents about data privacy and how the City utilizes data. This can be done by creating materials that outline data privacy precautions residents can make and distributing these materials at community events. Specific events around data privacy can also be held to engage residents on their data privacy rights. Staff should consult and engage communities most impacted by the potential use of technologies, like BIPOC and immigrant communities, in their community engagement efforts.

Outreach to the public may also include gathering public comment on PIAs and Proposed Use Policies and using the feedback gathered to review a PIA or proposed use policy before it is formally published.

The City of Portland has planned data privacy events where residents can learn about Digital Justice, Digital Rights, and Surveillance Technologies. They have also created a Community Leads Campaign where they are contracting (in practice, subcontracting) community organizers to directly guide the public outreach around data privacy and surveillance.

*Resources Required*

This will require TID staff to create materials and a curriculum around data privacy that will engage residents. Creating these materials can be done by existing TID staff or an intern. After this, TID staff should identify events and opportunities to share these resources requiring coordination with other City events and the creation of specific data privacy events.

*Level of Effort and Time Commitment*

Identifying data privacy resources and creating materials can take around 2 to 3 months. After the creation of the resources, they should be distributed and promoted to residents on an ongoing basis which will require TID staff time. Beyond this, planning data privacy specific events will be an ongoing effort.

*Guidelines Covered*

This recommendation covers Data Privacy Guidelines 2 and 3.

### 10. Educating Staff on Data Privacy

*Description*

To implement the Data Privacy Guidelines throughout the City, staff must be aware of the guidelines and measures they can take to protect residents' data. This can be accomplished through annual training and capacity building such as an Annual Security and Awareness Training. Online training materials about data privacy can also be distributed to employees instead of a workshop/meeting. Ultimately, educating staff on data privacy (and any related policies) will show them that taking data privacy precautions is not a roadblock to their work. The City of Seattle hosts an Annual Security and Awareness Training where they inform staff about how data privacy principles impact their work and their role in the data privacy programs.

*Resources Required*

This would require TID staff to coordinate and prepare training materials for City staff. There would need to be proper video-conferencing tools to host a large training as well.

*Level of Effort and Time Commitment*

This recommendation requires organizational buy-in to coordinate a City-wide training. TID Staff would need to identify which staff from each Department would benefit most from this type of workshop. Preparing and distributing electronic training materials would also require TID staff time to create the documents and Citywide coordination to distribute them to staff. This requires an ongoing annual effort from TID staff to update training materials.

*Guidelines Covered*

This recommendation covers Data Privacy Guidelines 4 and 5.

## 11. Data Privacy Website

*Description*

A data privacy website can serve as a central page to inform the community on what work is being done around the Data Privacy Guidelines. This website will increase transparency about data privacy in the City and can serve as a hub for data privacy resources. The City of Oakland utilizes a centralized website to post all Privacy Impact Assessments and Use Reports. The City of Seattle has a more robust data privacy website including Privacy Impact Assessments and other data privacy initiatives.

*Resources Required*

This will require TID staff to create a new webpage for data privacy, and input resources and updates about data privacy on the webpage. The webpage will require maintenance on a regular basis.

*Level of Effort and Time Commitment*

A data privacy website will require support from existing TID staff. The process of creating the website can take around 1-2 months and should be updated regularly to reflect data privacy work.

*Guidelines Covered*

This recommendation covers Data Privacy Guidelines 1, 2, and 3.

## 12. Implement Technology to Prevent Data Loss

*Description*

Data loss prevention (DLP) software, also known as data leak prevention software, is used to secure control and ensure compliance of sensitive information. A key component of DLP solutions is distribution control, which ensures users do not send private information outside of organizational networks. Security staff and network administrators set organizational rules that determine who can view, change, and share confidential data. DLP tools often control data on both the network and endpoint level to ensure policies remain consistent across the company. These tools are used to ensure the protection of data and prevent leaks by internal sources.

There are overlaps between DLP tools and some governance, risk & compliance (GRC) software, but these tools are specifically geared toward data control. Governance, risk, and compliance software are used to manage the flow and accessibility of information within an organization. GRC software can be used to identify risks, implement policies, and track compliance.

*Resources Required*

This will require TID staff to request the purchase of this software and identify the best DLP software for the organization. TID staff will then need to implement the software and educate staff on its purpose.

*Level of Effort and Time Commitment*

This will likely need to go through the RFP process and may take several months to select a software. There will need to be time allotted to allow for the implementation of the software.

This recommendation covers Data Privacy Guidelines 1 and 5.

## Recommendations' Impact and Feasibility

To help understand the impact and feasibility of the proposed recommendations, each recommendation has been evaluated for its community and internal impact, as well as it cost effectiveness and implementation feasibility. This can help staff prioritize how to implement these recommendations.

| Recommendation | Overall Impact | Overall Feasibility |
|---|---|---|
| Hiring Data Privacy Staff | Highest Impact | Low Feasibility |
| External Privacy Advisory Commission | High Impact | Medium Feasibility |
| Data Privacy Guideline Implementation Workgroup | Low Impact | Medium Feasibility |
| Surveillance Ordinance | Highest Impact | Medium Feasibility |
| Privacy Impact Assessments | Highest Impact | Medium Feasibility |
| Proposed Use Policies | Highest Impact | Medium Feasibility |
| Guidelines for Data Collection | High Impact | Highest Feasibility |
| Implement Data Privacy in the Procurement Process | High Impact | Highest Feasibility |
| Community Education Campaigns | High Impact | High Feasibility |
| Educating Staff on Data Privacy | High Impact | Medium Feasibility |
| Data Privacy Website | Medium Impact | High Feasibility |
| Implement Technology to Prevent Data Loss | Medium Impact | Low Feasibility |

## Next Steps

Implementing the Data Privacy Guidelines is largely dependent on City staff capacity. Understanding this, the Technology and Innovation Department (TID) plans to ask for the addition of a Data Privacy staff member (Recommendation #1) in the FY 23 budget. The addition of at least one staff member dedicated to data privacy will add focused staff capacity and increase the feasibility of implementing the following high-impact recommendations: External Privacy Advisory Commission, Surveillance Ordinance, Privacy Impact Assessments, Proposed Use Policies, and Implement Technology to Prevent Data Loss.

Even without the additional staff member, existing TID staff is dedicated to continuing to advance the Data Privacy Guidelines Implementation Plan. Staff is already making progress on developing Guidelines for Data Collection and Implementing Data Privacy in the Procurement Process. Additionally, the City's existing Data Policy Steering Committee Workgroup can be utilized as the Data Privacy Guideline Implementation Workgroup, and staff will continue to consult with the Technology & Innovation Commission on implementation of the Data Privacy Guidelines. Recommendations that do not necessarily require additional staff include Community Education Campaigns, Educating Staff on Data Privacy, and creating a Data Privacy Website; however, work on these will occur at a slower pace without the addition of a dedicated Data Privacy staff member.

# Best Practice Research
National Institute of Standards and Technology (NIST) Privacy Framework

[NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management](#)

The NIST Privacy Framework helps organizations build better privacy foundations by bringing privacy risk into parity. The NIST Privacy Framework can be utilized to implement privacy risk management in the organization. When used as a risk management tool, the Privacy Framework can assist an organization in its efforts to optimize beneficial uses of data and the development of innovative systems, products, and services while minimizing adverse consequences for individuals. The Privacy Framework can help organizations answer the fundamental question, "How are we considering the impacts to individuals as we develop our systems, products, and services?" When implementing these recommendations, the NIST Privacy Framework can help to ensure the programs, procedures, and processes built protect the individual and the organization.

## Privacy Impact Assessments
### Federal Government Practices
The Department of Justice released Privacy Impact Assessment (PIA) guidance for [State, Local, and Tribal Justice Entities](#). A PIA aids in privacy policy development by allowing organizations analyze privacy risks and exposures of data storage and information sharing. Policies following the PIA should address these privacy risks.

A PIA should be conducted to evaluate privacy implications when information systems are created, when existing systems are significantly modified, and also at any other time.

The Department of Education's [PIA inventory](#), provides examples of the agency's PIAs and guidance on what a PIA should include.

The objectives of a PIA include:

- Provide a tool to make informed policy and system design or procurement decisions based on an understanding of privacy risks and options available for mitigating these risks.
- Ensure that system and program managers are accountable for the proper handling of privacy issues.
- Establish a consistent format and structured process for analyzing both technical and legal compliance with applicable privacy laws and regulations, as well as accepted privacy policy.
- Provide basic documentation on the flow of personal information within systems for use and review by policy, program, and management staff; systems analysts; and security specialists.
- Provide the public with assurances that their personal information is protected.

### Local Government Practices
Local governments use tools similar to PIAs to identify privacy risks and communicate with these risks to the public.

*City of Seattle*
The City of Seattle's issues Surveillance [Impact Reports](#) (SIR) and [Privacy Reviews](#),

There are several steps the City of Seattle takes to review surveillance technologies. This process allows for the staff to review policies, identify surveillance data risks, and gain public feedback.

1. Upcoming for review: This stage denotes that the technology is upcoming for review, but the department has not begun drafting the Surveillance Impact Report (SIR).
2. Initial draft: Research and documentation about the technology is drafted and compiled during this stage.

3. Public Comment: The initial draft of the SIR and supporting materials have been released for public review and comment. During this time, one or more public meetings will take place to solicit feedback.
4. Final draft: During this stage the SIR, including collection of all public comments related to the specific technology, is being compiled and finalized.
5. Working Group: The Surveillance Advisory Working Group will review each SIR final draft and complete a Civil Liberties and Privacy Assessment, which will then be included with the SIR and submitted to Council.
6. SIR finalization: During this stage the final SIR is being compiled, including the CTO Response to the Working Group's Privacy and Civil Liberties Impact Assessment, fiscal note, and drafted legislation.
7. Council Review: The technology is transmitted to City Council for review and determination for use.

The City of Seattle also uses Privacy Impact Assessments (PIA) to conduct in-depth privacy reviews of a programs or projects.

PIAs ask questions about the collection, use, sharing, security and access controls for data that is gathered using a technology or program. They also request information about policies, training and documentation that govern use of the technology. The PIA responses are used to determine privacy risks associated with a project and mitigations that may reduce some or all of those risks.

To promote transparency, the City of Seattle publishes all PIAs on their website.

The City of Seattle conducts a PIA in two circumstances.

– When a project, technology, or other review has been flagged as having a high privacy risk.
– When a technology is required to complete the Surveillance Impact Report process. This is one deliverable that comprises the report.

The City of Seattle uses a PIA template and guidelines to create a standard for their PIAs. Guidelines include that reports must be drafted without the use of acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, the City of Seattle requires that PIAs principally use non-technical language to ensure they are accessible to audiences unfamiliar with the topic.

### County of Santa Clara
The County of Santa Clara issues Surveillance Assessments, for new technologies used by the County. Surveillance Assessments are approved by the Board of Supervisors. The Surveillance Assessments include these sections:

1. Purpose
2. Authorized and Prohibited Uses
3. Data Collection
4. Data Access
5. Data Protection
6. Data Retention
7. Public Access
8. Third-Party Data-Sharing
9. Training
10. Oversight

### City of Oakland
The City of Oakland issues Impact Reports and Use Policies for new technologies.

Impact reports include these sections:

1. Information Describing the Technology and How it Works
2. Proposed Purpose
3. Locations of Deployment
4. Potential Impact on Civil Liberties and Privacy
5. Mitigations
6. Data Types and Sources
7. Data Security
8. Fiscal Cost
9. Third Party Dependence
10. Alternatives
11. Track Record

Use policies include these sections:

1. Purpose
2. Authorized Use
3. Data Collection
4. Data Access
5. Data protection
6. Data retention
7. Public Access
8. Third-Party Data-Sharing
9. Training
10. Auditing and oversight
11. Maintenance

## Privacy Matrices

Creating a data risk classification matrix is another tool to assess risk. A data risk matrix classifies information assets into risk categories to determine who may access the information and what minimum security precautions must be taken to protect it against unauthorized access.

[University of Pittsburgh Data Risk Classification and Compliance](#)

[Monash University Privacy Matrix](#)