

Utah Office of Data Privacy – Privacy Awareness Training

Last Revised: 6/1/2025



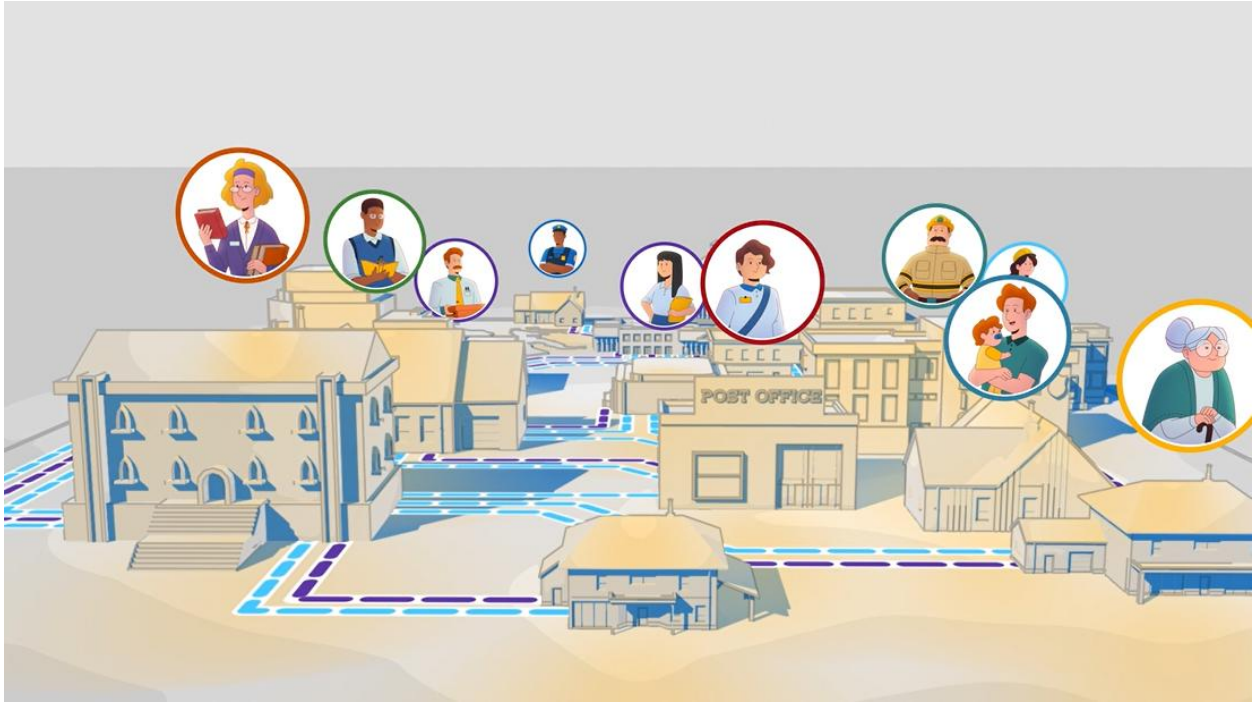
Data Privacy Awareness Training

privacy.utah.gov

Welcome to the Data Privacy Awareness Training. In the next few minutes, we'll explore what data privacy is, how it impacts us, and how we can all play a part in protecting it.



Privacy is a core value in Utah's history and remains crucial in today's digital age.



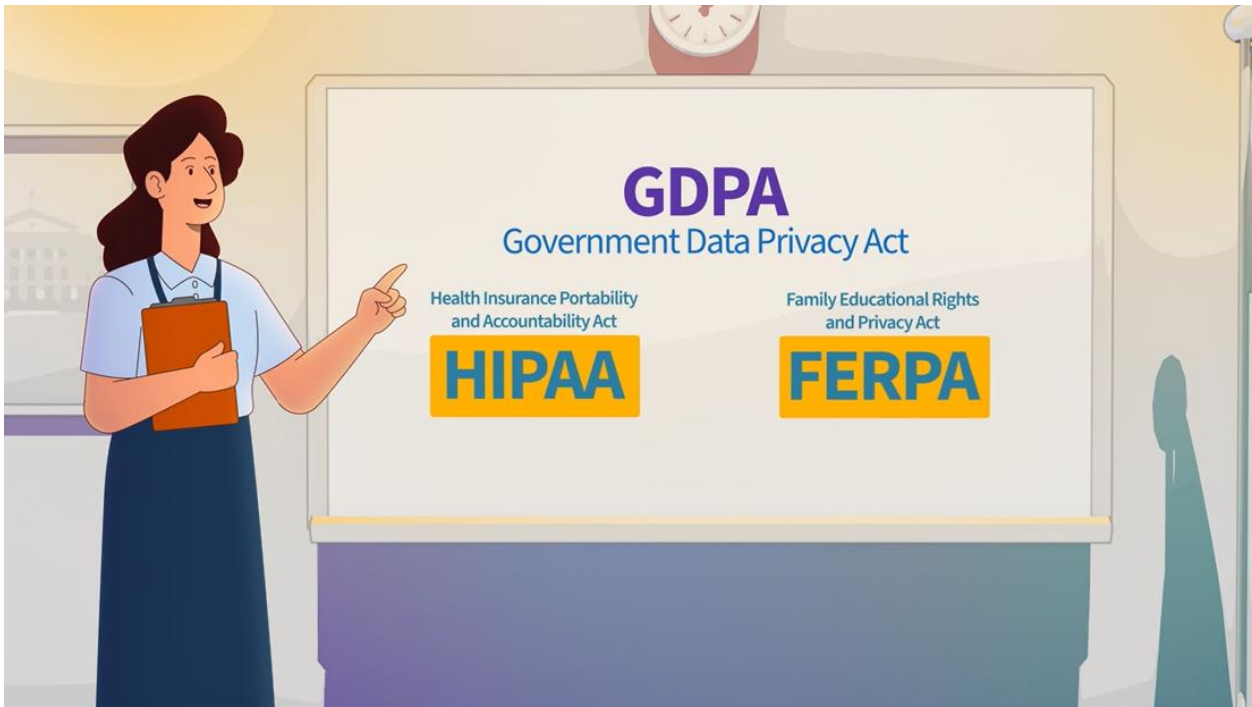
Governmental entities at all levels in Utah must uphold data privacy to protect citizens' interests, foster trust in public services, and ensure transparency and accountability.



All governmental entities are subject to baseline data privacy requirements...



...established in the Government Data Privacy Act, which we refer to as GDPA.



In addition, some entities are subject to more specific or restrictive regulations like the Health Insurance Portability and Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act (FERPA).



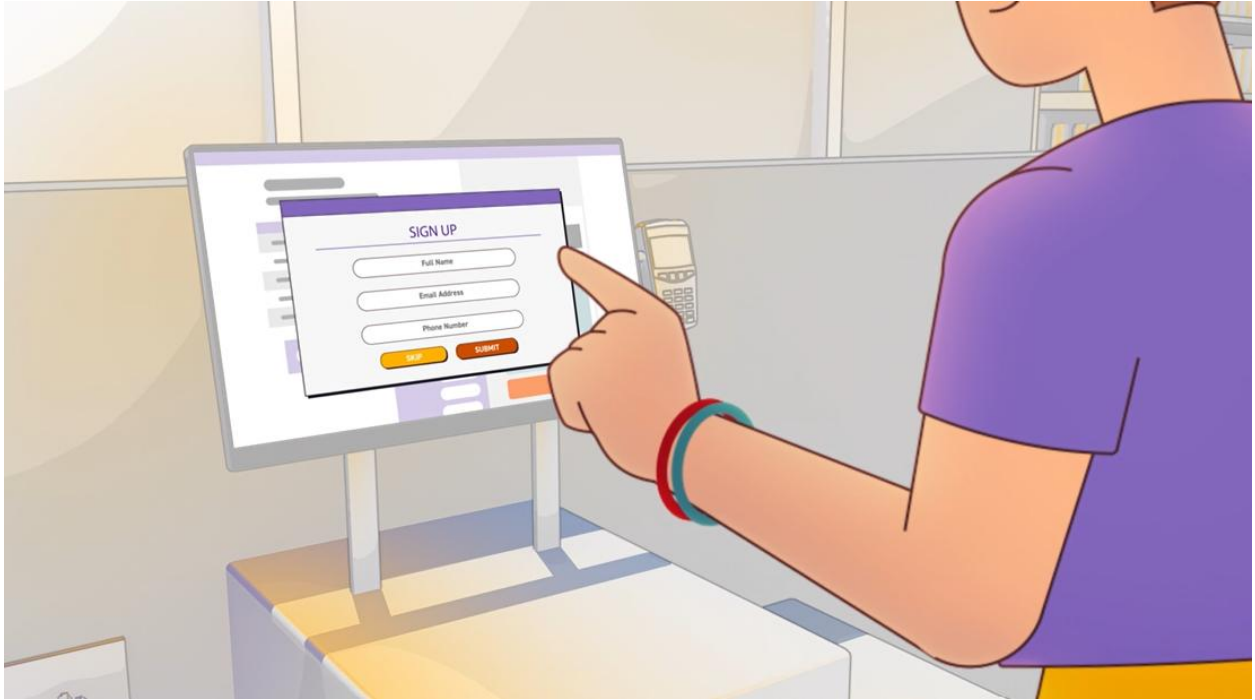
Entities must understand and comply with privacy obligations to safeguard personal data and maintain public trust.



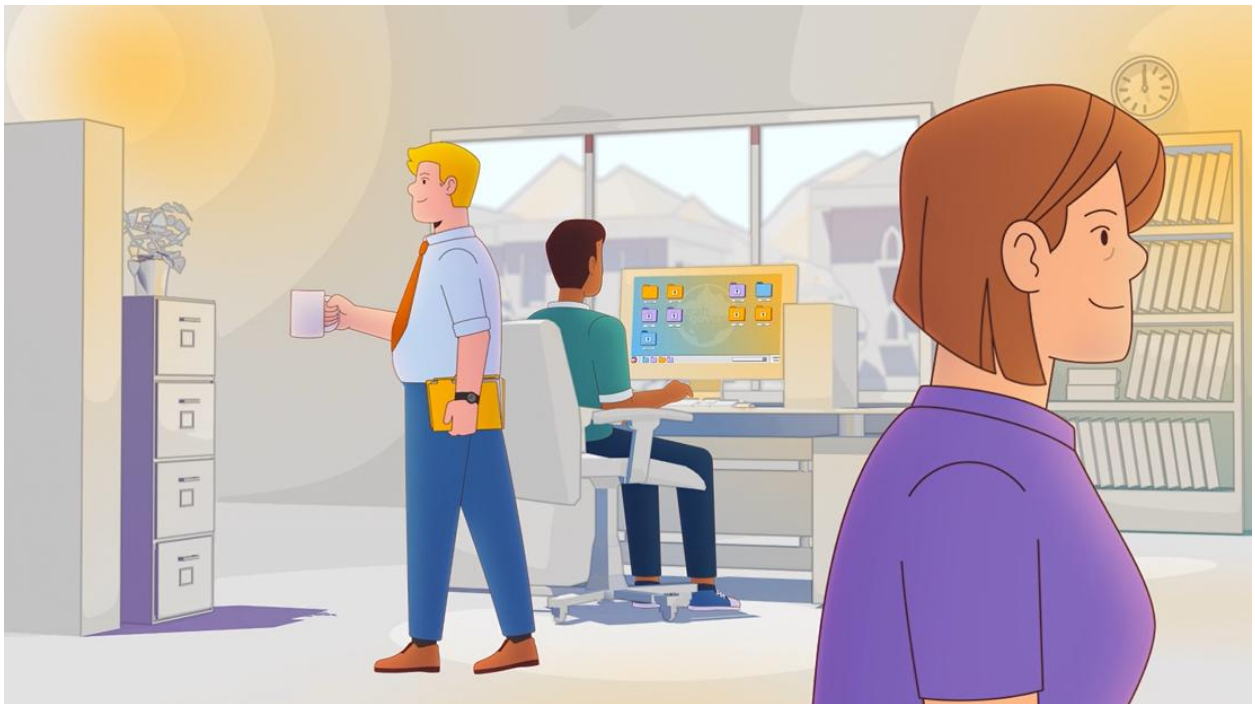
What is Data Privacy?

privacy.utah.gov

What is Data Privacy?



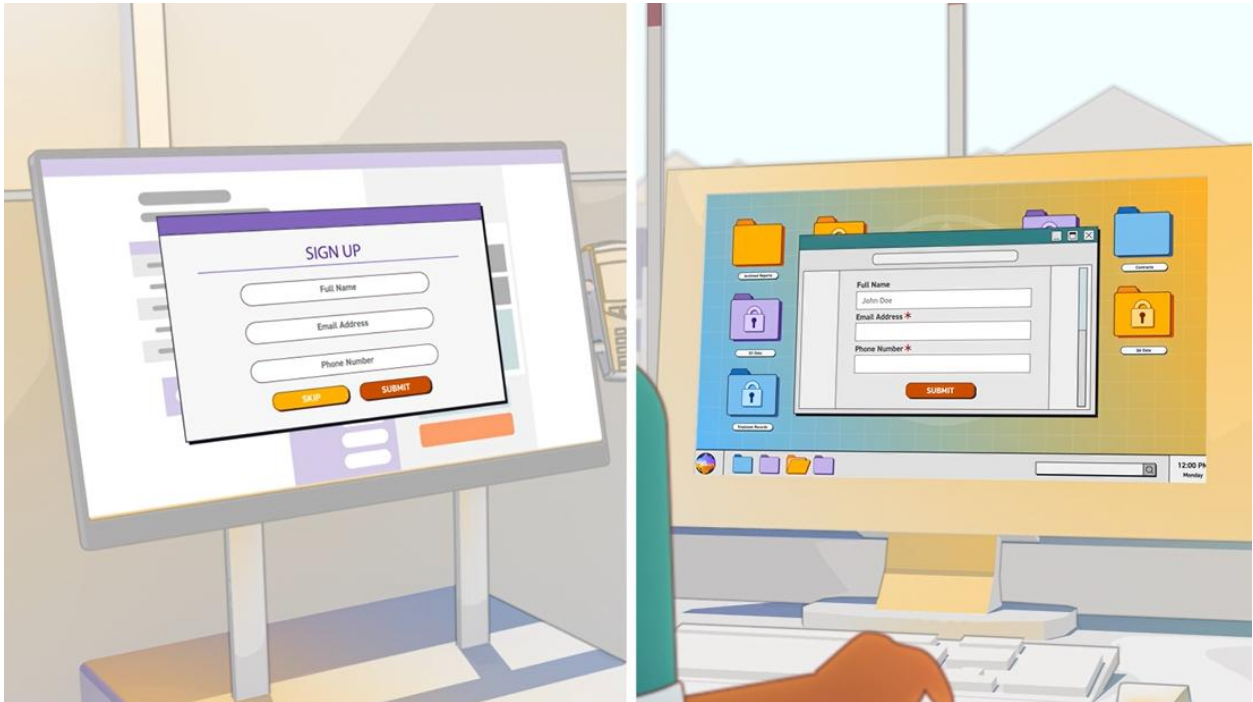
In the private sector, we often have the ability to choose what happens with our personal data.



But when it comes to government services, we don't always have the same type of control.



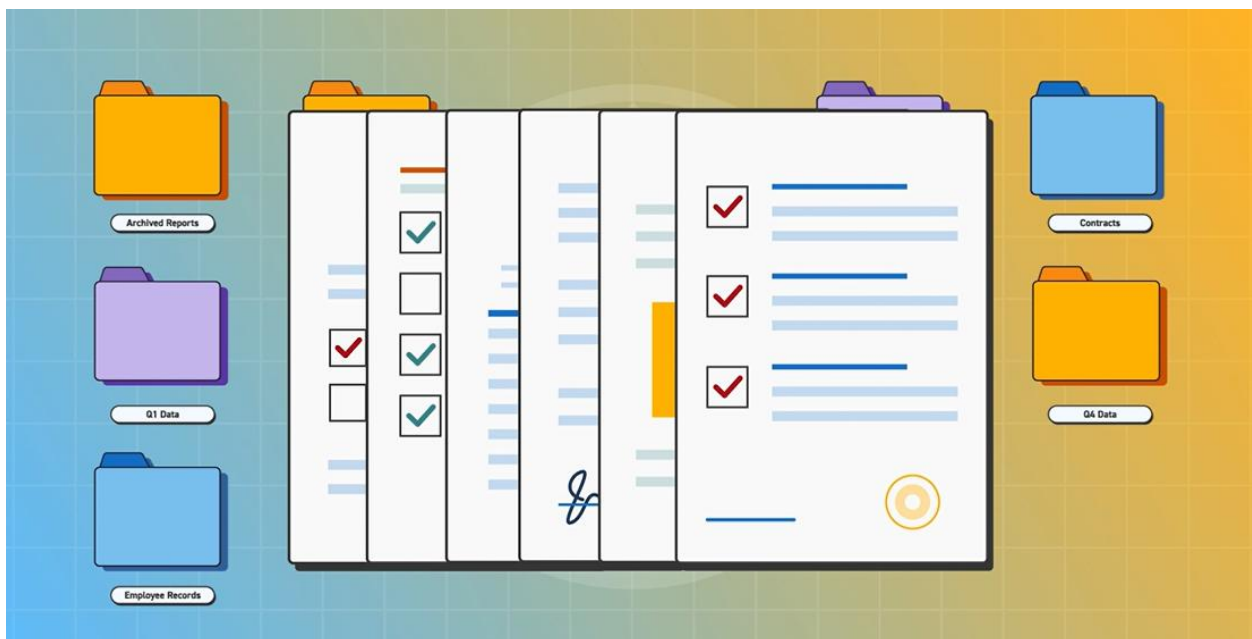
Either we provide our personal data to access important services, or we go without them.



This contrast highlights the importance of data governance and its relationship to privacy.



Data privacy refers to the protection and responsible management of personal data, ensuring that it is collected, accessed, used, and disclosed only as authorized.



It safeguards an individual's control of their personal data--such as financial details, health information, and online activity-



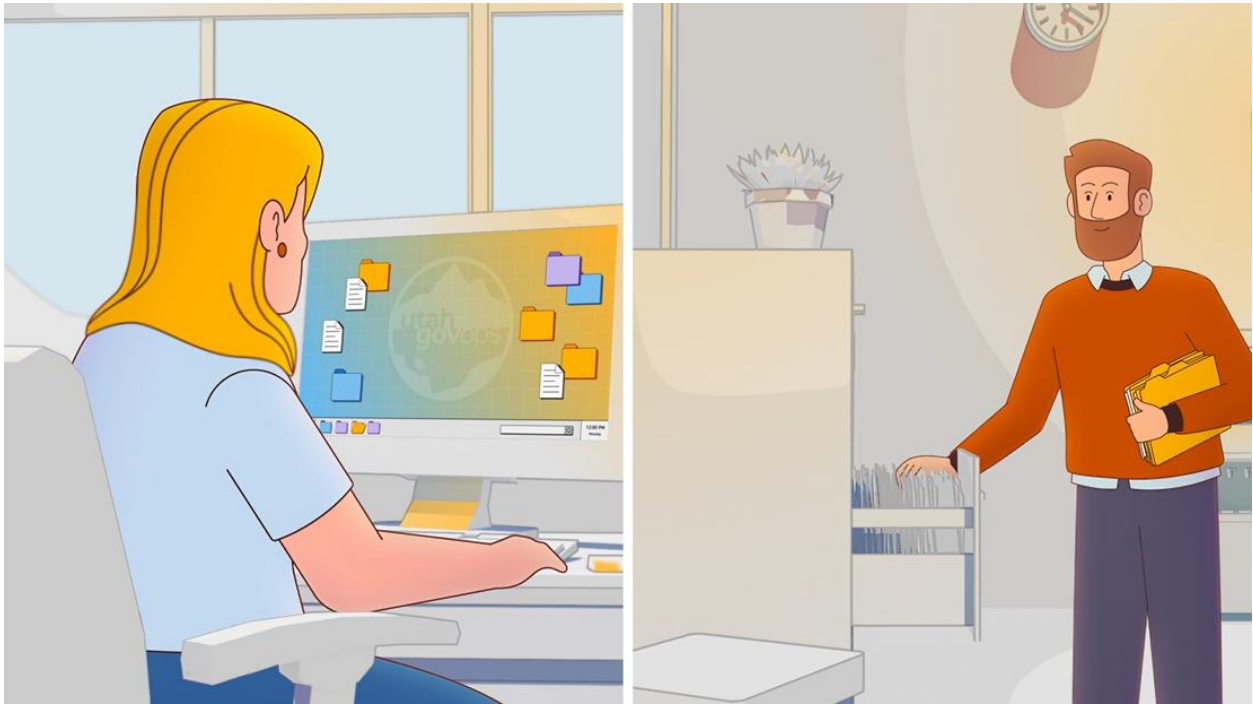
...so the data is kept secure and used only for authorized purposes.



GDPA plays a crucial role in data privacy by creating baseline requirements in law that govern how personal data should be collected, stored, used, and shared by governmental entities.

How does Records Management relate to Data Privacy?

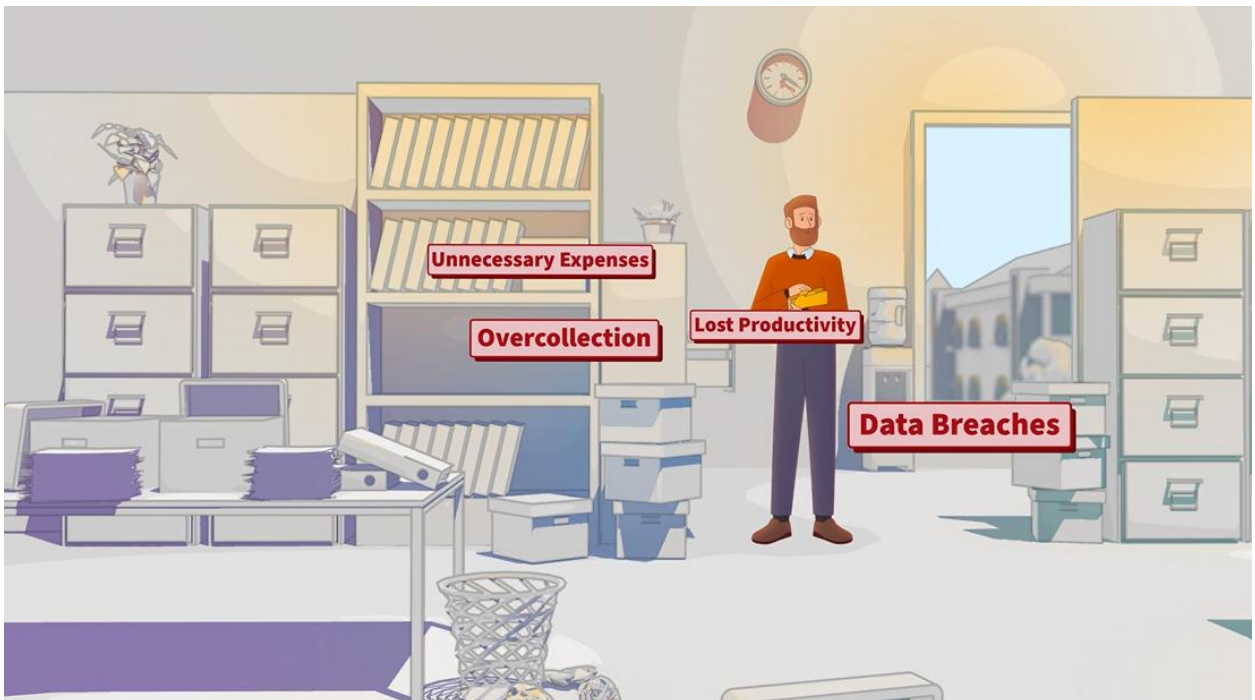
privacy.utah.gov



Data privacy is tied to the records we create – from physical documents to digital data. Collecting personal data can be easy, but managing it is much harder.



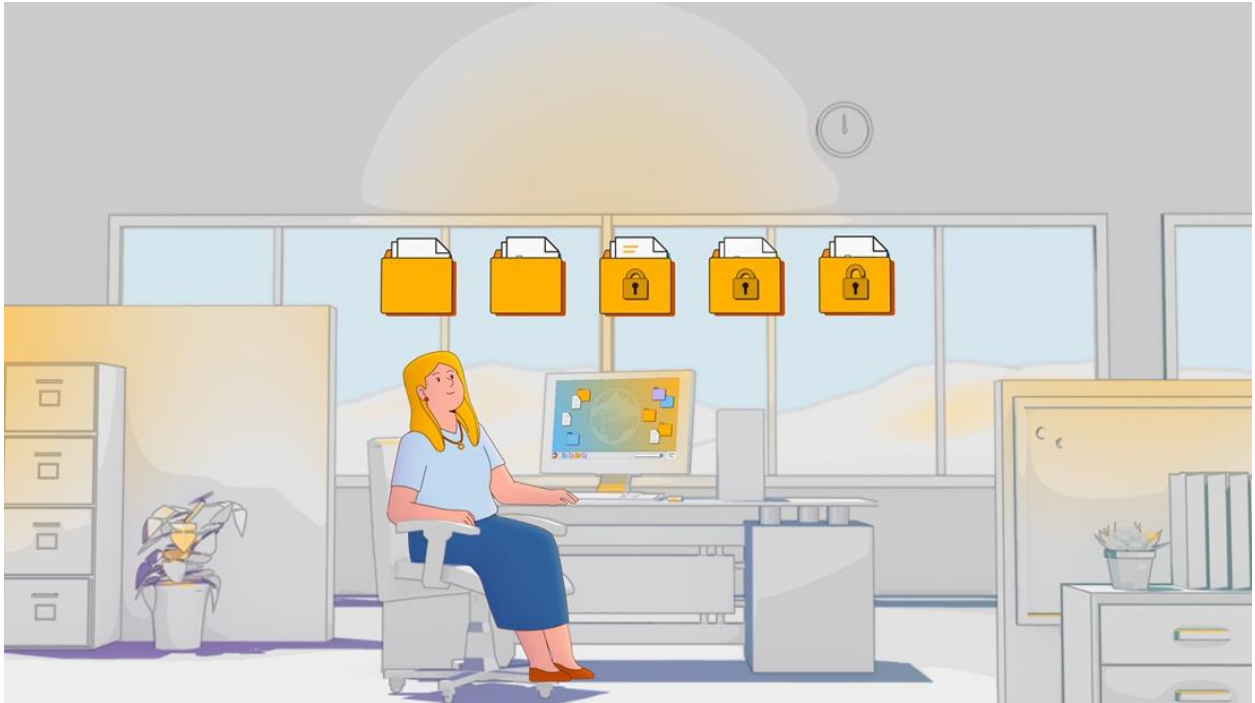
Without proper records management, from the collection of personal data to its disposal, government entities are likely to see-



...lost productivity, unnecessary expenses, overcollection, and possibly even data breaches.



Governmental entities must classify and organize records to safeguard an individual's data privacy.



Records must be managed according to their record series attributes, for example, how long they need to be kept, how sensitive they are, and what they are used for.



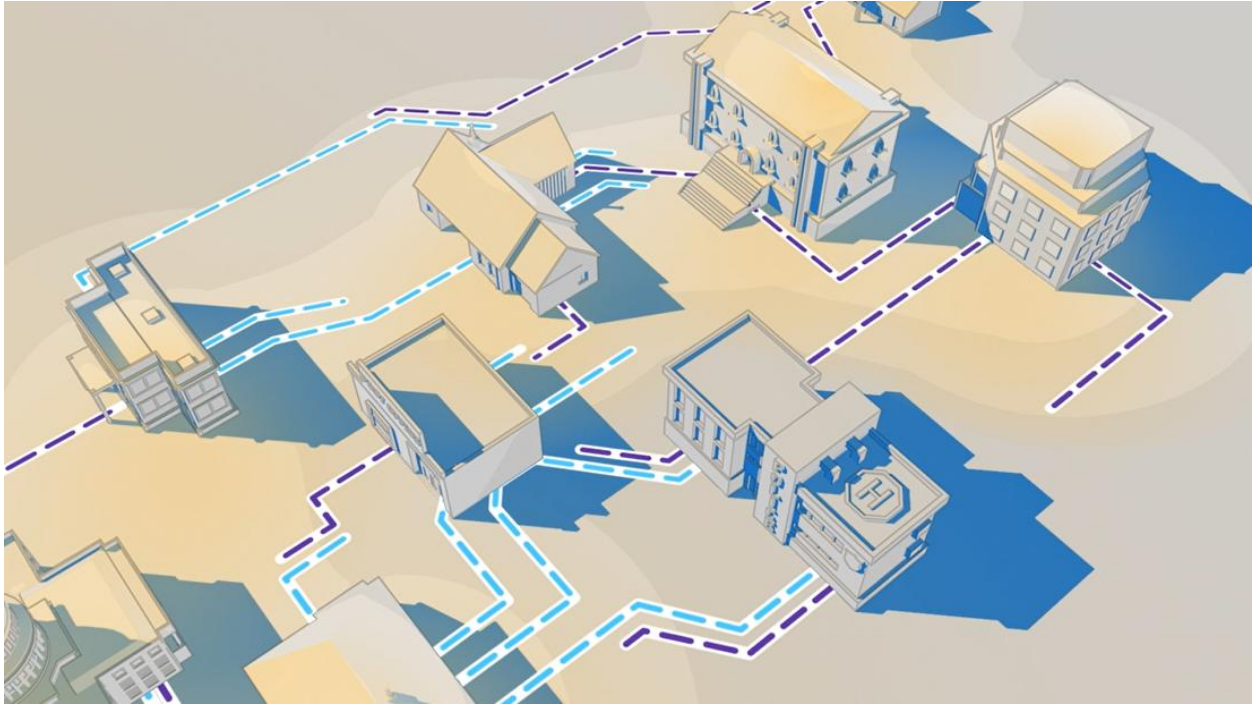
Proper records management protects data privacy and transparency while allowing your entity to effectively use personal data to provide essential services.



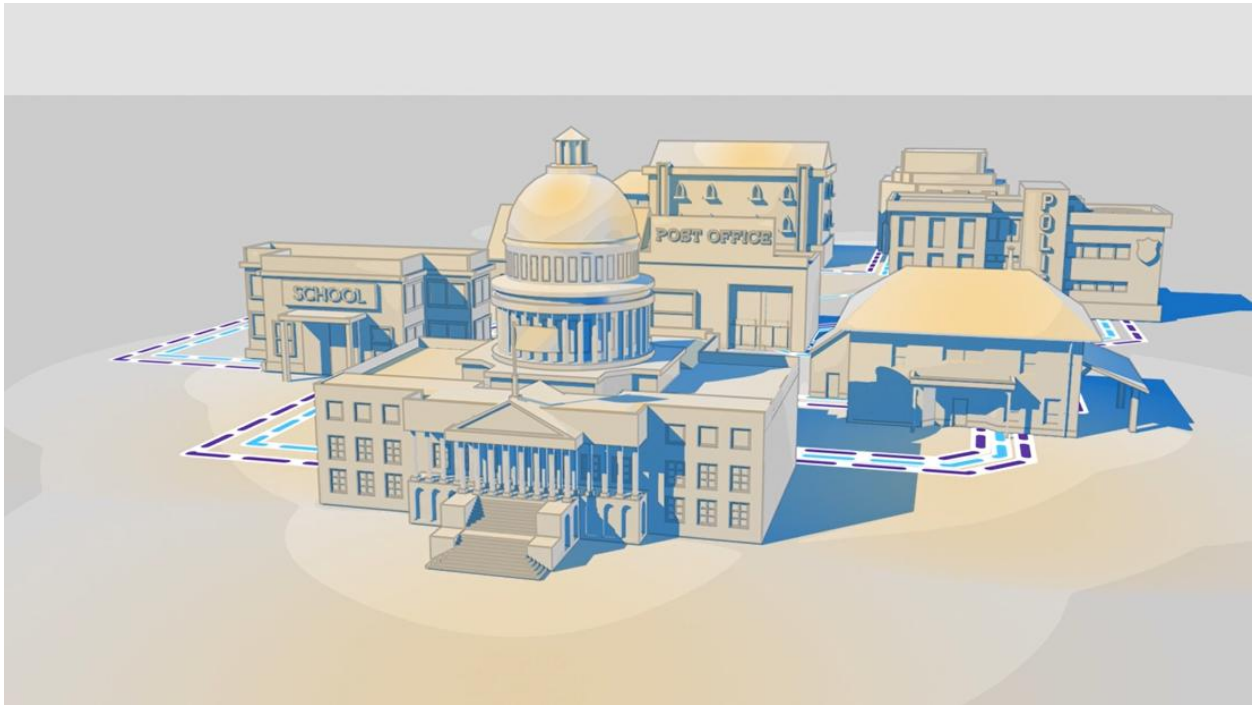
Data Privacy Obligations for Government

privacy.utah.gov

Data Privacy Obligations for Government



Protecting an individual's personal data helps build trust between the public and government.



Every governmental entity in Utah is required to initiate a data privacy program.



This program is the framework by which your entity will implement data privacy practices that fulfill their data privacy obligations.



Data privacy practices include safeguards to protect personal data, meet legal requirements, and inform individuals about their data privacy interests.



The data privacy program of each governmental entity should be customized to meet its specific requirements, while accounting for the baseline standards set by the GDPR.



Data Privacy Obligations for Government

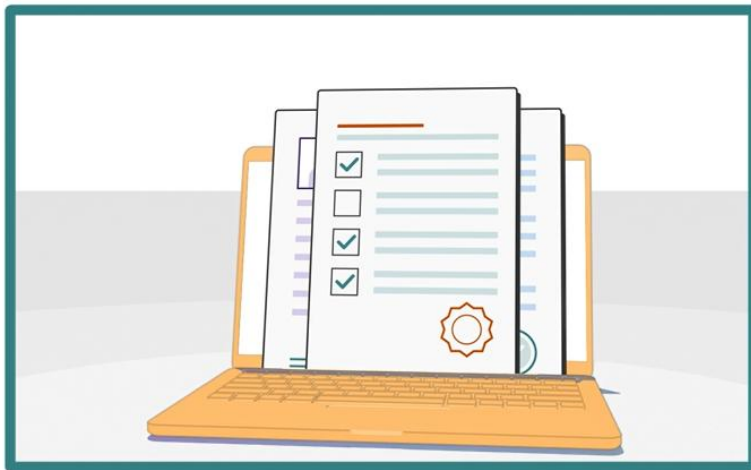
privacy.utah.gov

Here are some examples of privacy practices your privacy program may include:



Designate Chief Administrative Officers

Designating a Chief Administrative Officer who will be responsible for overseeing the governmental entity's data privacy program.



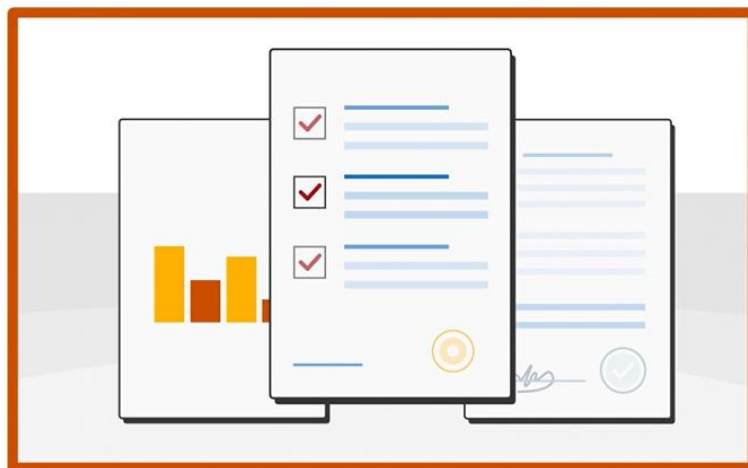
Inventory of Processing Activities

Conducting an inventory of all the personal data collected and processed by the governmental entity.



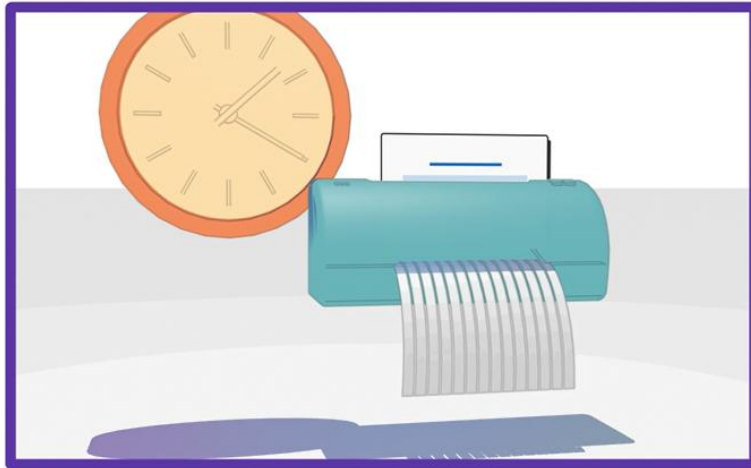
Privacy Notice

Providing a clear data privacy notice on forms when collecting personal data or user data.



Data Minimization

Ensuring that only the minimum amount of personal data is collected to achieve the governmental entity's purposes.



Retention and Disposition of Records Containing PII

Disposing of personal data according to approved retention schedules to ensure that personal data is not retained longer than necessary.



Breach Notification

Providing notice of a data breach to impacted individuals.



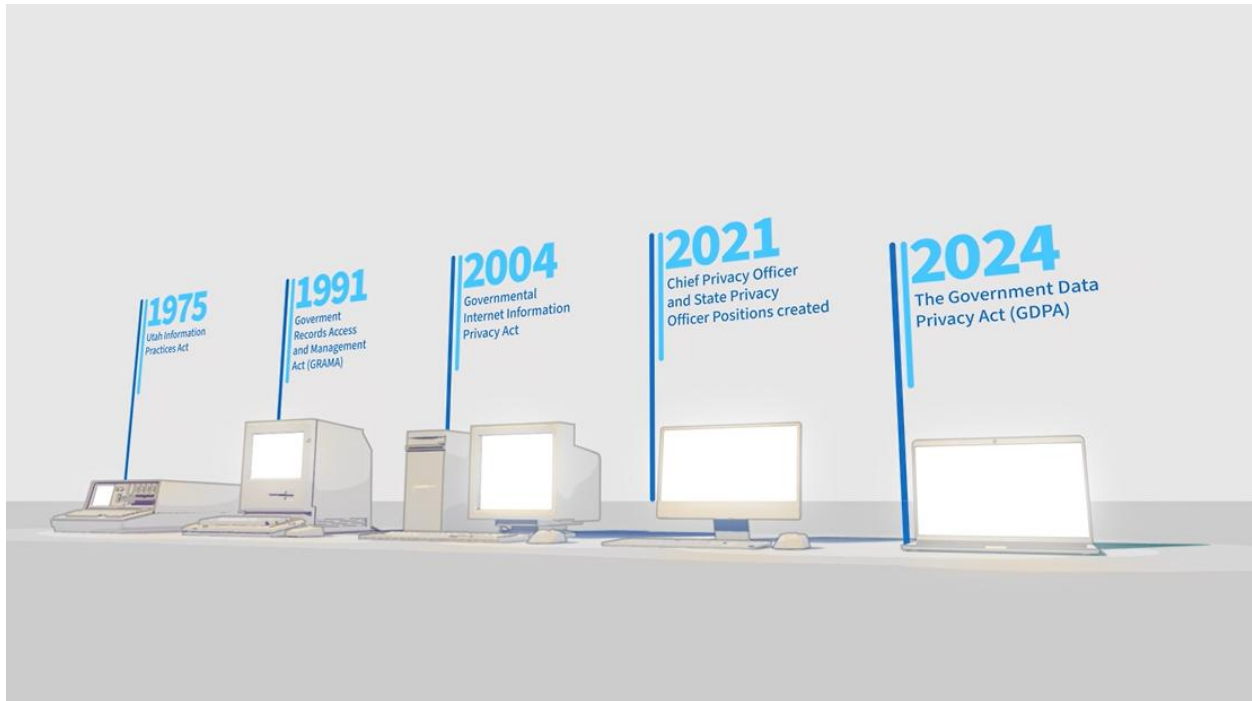
Data privacy practices like these provide a strong foundation for your data privacy program. You should contact your entity's Chief Administrative Officer if you are unaware of what data privacy practices you should be following. You can learn more about these and other generally applicable data privacy practices by visiting privacy.utah.gov.



Utah's Forward-Looking Strategy

privacy.utah.gov

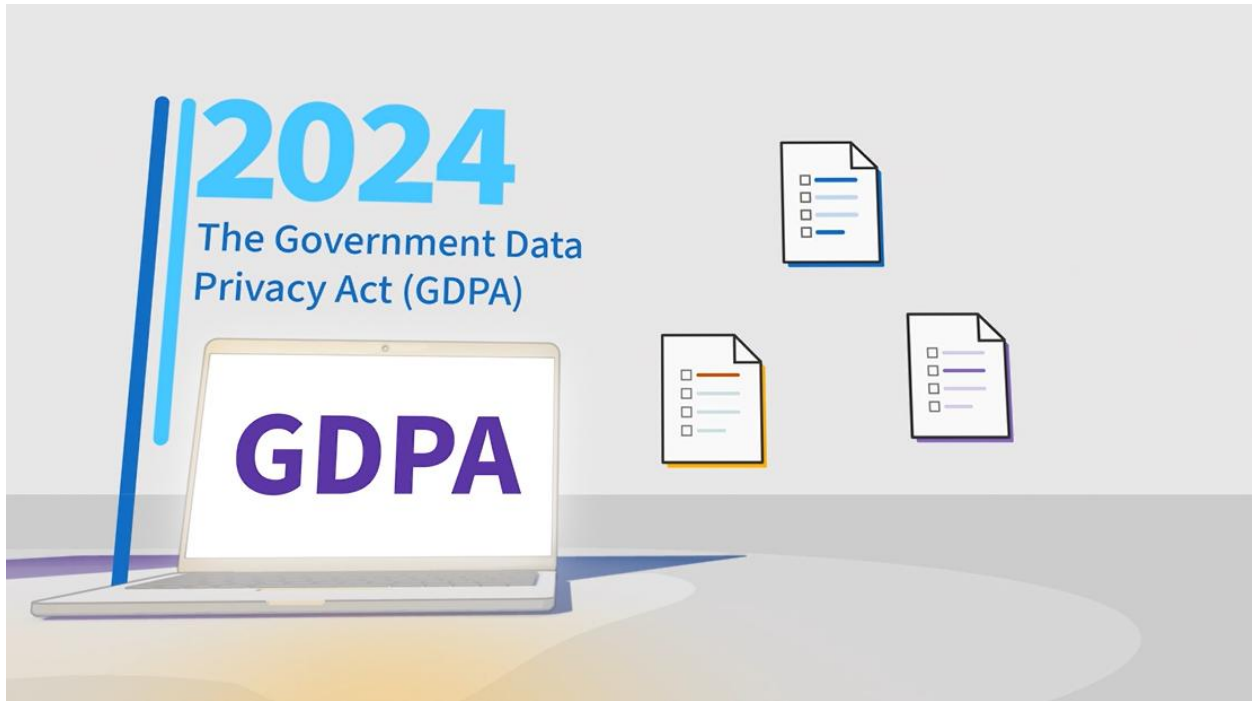
Utah's Forward-Looking Strategy



Many of the data privacy practices have existed in various parts of Utah law for over 30 years. As technology has advanced, some of these obligations have not been fully implemented by governmental entities.



The Government Data Privacy Act (GDPA) establishes a forward-looking strategy that helps address such gaps.



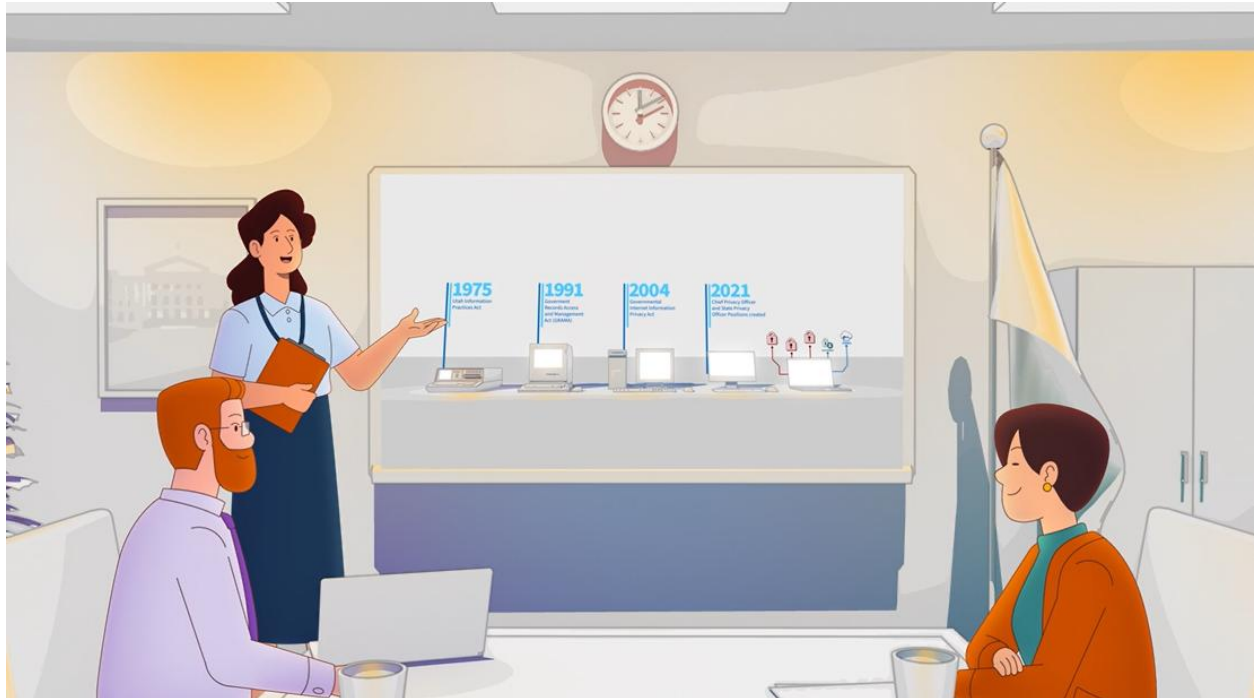
All new processing activities implemented by governmental entities must be compliant with the requirements in the GDPA.



Processing activities may include: how the data is collected, organized, altered, accessed, or stored. For pre-existing processing activities, entities are required to document areas of noncompliance and develop strategies to bring those activities into compliance.



This proactive approach ensures that Utah remains a leader in protecting individual's data privacy while considering resource allocation and prioritization. It will take many years to build mature data privacy programs and processes,

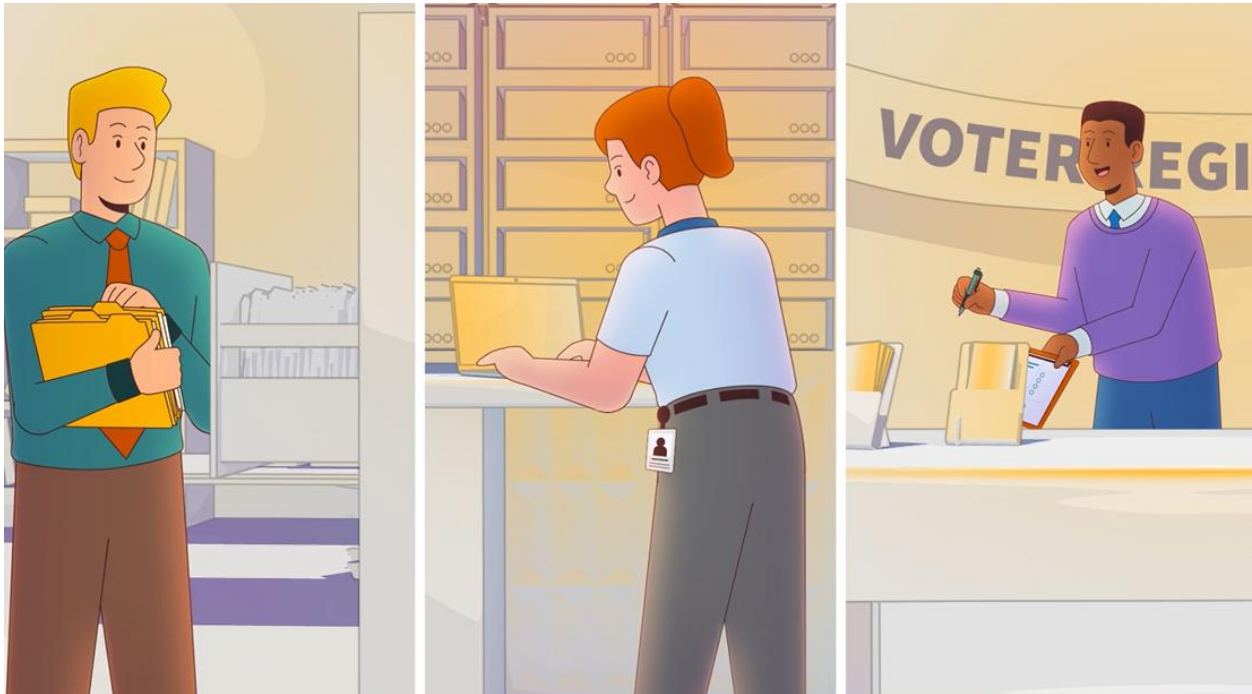


...but with consistent and disciplined efforts, all governmental entities in Utah will be leaders in data privacy.

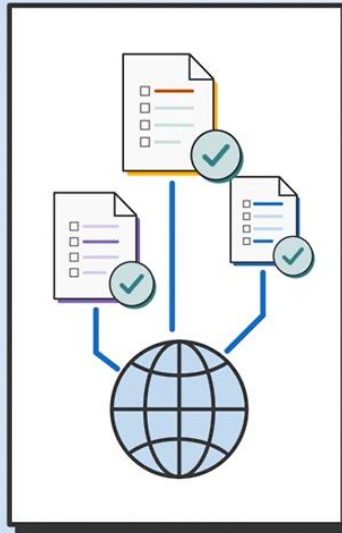
Your Role in Data Privacy

privacy.utah.gov

Your Role in Data Privacy



As a government employee who processes personal data in your daily work, whether it's handling forms, maintaining IT systems, or providing services, your actions directly impact data privacy. Here's how you can contribute to protecting an individual's data privacy:



Collecting Personal Data through Online Forms

Best Practice: Minimize the amount of data collected, obtain clear consent, provide a personal data collection notice, encrypt the information

Common Tasks Involving Personal Data. Collecting personal data through online forms

Best Practice: minimize the amount of data collected, obtain clear consent, provide a personal data collection notice, encrypt the information

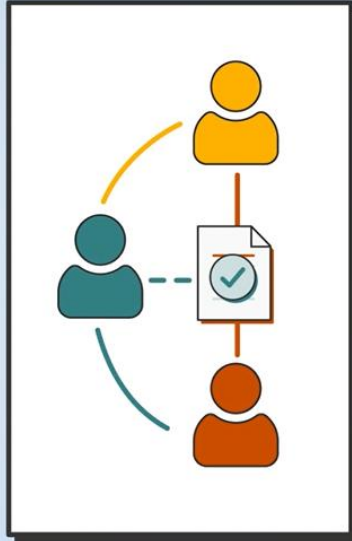


Storing Personal Data in a Database

Best Practice: Restrict access to personal data to authorized personnel only, Establish clear data retention policies that define how long personal data will be stored and how it should be used, Conduct regular audits to detect vulnerabilities

Storing personal data in a database. **Best Practice:** Restrict access to personal data to authorized personnel only, Establish clear data retention policies that define how long

personal data will be stored and how it should be used, Conduct regular audits to detect vulnerabilities



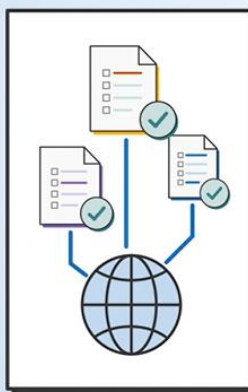
Sharing Personal Data with Third Parties

Best Practice: Enter into formal data sharing agreements, anonymize or pseudonymize personal data before sharing

Sharing personal data with third parties. **Best Practice:** Enter into formal data sharing agreements, anonymize or pseudonymize personal data before sharing

Common Tasks Involving Personal Data

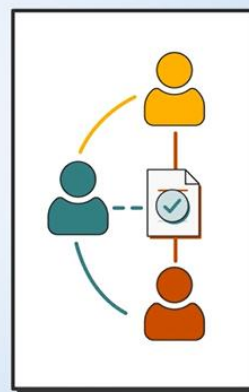
COLLECT



STORE & USE



SHARE



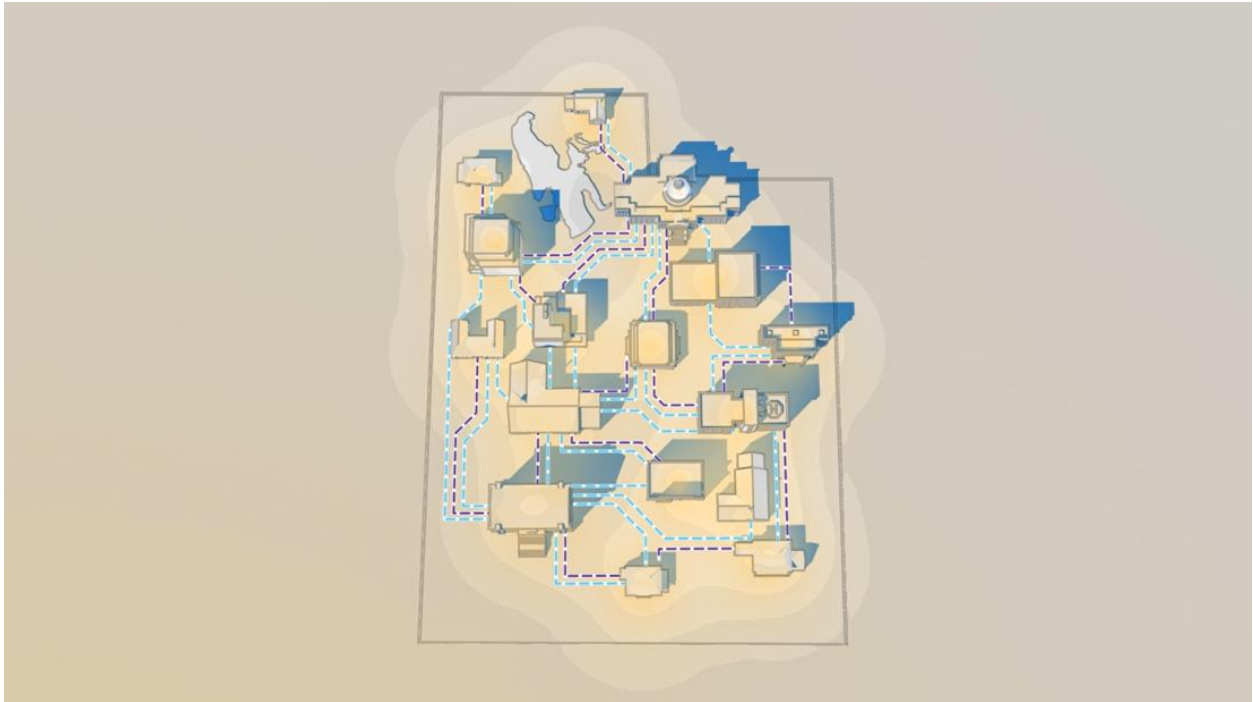
Small actions, like updating outdated forms or reporting potential risks, contribute to a privacy-conscious culture.



Conclusion: Now that you understand the importance of data privacy, remember that we all have a responsibility to protect personal data.



By following the practices outlined in GDPR, we strengthen trust in our systems and protect individuals' data privacy interests.



At the Utah Office of Data Privacy, we're here to assist in prioritizing data privacy.



office of
Data Privacy

Protecting Privacy, Protecting Trust

privacy.utah.gov

Together, we can build a more secure and trusted government for all. Thank you for watching. For more information, visit privacy.utah.gov.