Utah Division of Archives and Records Service

GUIDELINE FOR MANAGING DATA WHEN USING A THIRD-PARTY VENDOR

February 2021

PURPOSE: This guideline introduces basic considerations that governmental entities need to address when using a third-party vendor to execute a business process or function of the entity (including managing its records), to do work on behalf of the entity, or act as an agent of the entity.

The Division of Archives and Records Service is providing this guideline to help government agencies protect themselves from cyber threats or data loss, and to protect the public's interest in privacy as well as in government transparency.

Contents

Definitions

Contractor

A person who contracts with a governmental entity to provide goods and services directly to a governmental entity.[1]

Private Provider

A person who contracts with a governmental entity to provide goods and services directly to the public.[2]

Person

An individual, a nonprofit or profit corporation, a partnership, a sole proprietorship, other type of business organization, or any combination acting in concert with one another.[3]

Managed Service Provider (MSP)

An entity that delivers services, such as network, application, infrastructure and security, via ongoing and regular support and active administration on customers' premises, in their MSP's data center (hosting), or in a third-party data center. MSPs may deliver their native services in conjunction with other providers' services. The term MSP traditionally was applied to services centered on infrastructure or a specific device but has expanded to include any continuous, regular management, maintenance and support.[4]

GRAMA request

A request for records that is submitted to a Utah governmental entity per Utah Code 63G-2, Government Records Access and Management Act (GRAMA).

Ownership of Records

Records or data created on behalf of a governmental entity by a contractor or private provider are considered government records, unless explicitly stated otherwise in contract. This is implied in the legal definition of a record, per Utah Code 63G-2-103(22):

[1] Government Records Access and Management Act, Utah Code § 63G-2-103(5) (Supp. 2020). Accessed January 14, 2021. https://le.utah.gov/xcode/Title63G/Chapter2/63G-2-S103.html.

[2] Government Records Access and Management Act, Utah Code § 63G-2-103(18) (Supp. 2020). Accessed January 14, 2021. https://le.utah.gov/xcode/Title63G/Chapter2/63G-2-S103.html.

[3] Government Records Access and Management Act, Utah Code § 63G-2-103(17) (Supp. 2020). Accessed January 14, 2021. https://le.utah.gov/xcode/Title63G/Chapter2/63G-2-S103.html.

[4] Gartner. "Gartner Glossary, Information Technology Glossary, M, Managed Service Provider (MSP)." Gartner, Inc. Last modified January, 2021. Accessed January 14, 2021. https://www.gartner.com/en/information-technology/glossary/msp-management-service-provider.

(a) 'Record' means a book, letter, document, paper, map, plan, photograph, film, card, tape, recording, electronic data, or other documentary material regardless of physical form or characteristics

(i) that is prepared, owned, received, or retained by a governmental entity or political subdivision; and

(ii) where all of the information in the original is reproducible by photocopy or other mechanical or electronic means.[5]

If a contract stipulates that some records are owned by the contractor or private provider, it should also specify that those records are subject to GRAMA and the Public Records Management Act (PRMA). Conditions of a contract have to comply with state laws.

In a 2016 hearing, *Utah Rivers Council v. Washington County Water Conservation District* (2016-19), the State Records Committee (SRC) learned that a "third party was hired by Respondent to do work for Respondent, and the third party maintains the records as Respondent's agent. Therefore, the governmental entity owns and can obtain a copy of the records." The SRC found that "even though the records were maintained by a third party, Respondent was the owner of the records and therefore, the disputed records should be considered governmental records subject to GRAMA."[6] The agency was ordered to release the records to the requester; more importantly, this case made it clear that agency ownership can extend to records created by contractors and private providers when they are acting on the government's behalf, doing something that the government would otherwise be doing. Subsequently, agencies have responsibility to oversee the management of records created by vendors with which they contract.

Retention of Records

A government agency needs to have a retention schedule that applies to the records (including data) being created by a contractor or private provider.

Utah law requires that all government records be managed according to approved retention schedules, in accordance with Utah Code 63G-2-604, 63G-2-701 (in the case of political subdivisions who choose to create and adopt their own retention schedules), and 46-4-301 (specifically regarding electronic records). A retention schedule for records in the custody of a third-party vendor may be specific to those records, or may include those records as part of a larger grouping of records (also known as a "record series"). If an agency doesn't have a

[5] Government Records Access and Management Act, Utah Code Ann. §§ 63G-2-103(22) (Supp. 2020). Accessed January 14, 2021. https://le.utah.gov/xcode/Title63G/Chapter2/63G-2-S103.html.

[6] "State Records Committee Appeal Decision 2016-19." Utah Department of Administrative Services, Division of Archives and Records Service. Last modified May 23, 2016. Accessed November 18, 2020. https://archives.utah.gov/src/srcappeal-2016-19.html

retention schedule approved specifically for the third-party vendor records, the “model retention schedules,” or general retention schedules, maintained by the State Archives “shall govern the retention and destruction of that type of material.”[7]

Retention schedules allow for the legal disposition of data, whether through destruction or transfer. Disposing of data that have met retention is the cheapest, easiest way for an agency to keep their data secure and manageable. Ideally, plans for deleting or transferring data according to the retention schedule are specified in a contract with a third-party vendor, and methods for deleting or transferring data according to the retention schedule are built into the applicable content management system.

Access to Records

A government agency should have access to records that are created, collected, or retained as part of their business processes, even if a third-party vendor (contractor or private provider) is executing the process on their behalf.

When selecting or negotiating with a vendor, it’s important to find out how records will be accessed by those with the authority to do so. Will there be additional expense incurred for accessing or authenticating records? How will copies of the records be provided in response to audit or GRAMA requests? These situations should be addressed and provided for in the vendor contract.

Security of Records

When selecting or negotiating with a vendor, it’s also important to find out how records will be protected from unauthorized access. Research the supply chain of any vendor before contracting with them. What companies do they use or contract with to provide elements of their service further up or down the supply chain (a common practice with cloud services)? Are those companies secure?

Find out what processes the vendor uses to test the security of their systems and your data, and what protocols they have in place to handle data breaches.

This type of research should be built into a government agency’s cybersecurity processes and program. The following checklist provides additional questions that records officers or their technology services staff should be able to answer.

Cybersecurity Checklist[8]

- Do you have a risk profile?

[7] Government Records Access and Management Act, Utah Code Ann. §§ 63G-2-604(1)(c) (Supp. 2019). Accessed November 18, 2020. https://le.utah.gov/xcode/Title63G/Chapter2/63G-2-S604.html

[8] Ysasi, Andrew. *Cybersecurity and Information Governance (IG)*. October 15, 2020.

  - If so, how often is it updated?
  - Is the profile shared with insurance organizations and critical vendors?
- Do you have a data map?
- How current are your network diagrams?
- During the procurement process, do you feel your information security needs are being met?
- Do you have a DLP (Data Loss Prevention) policy?
  - If so, how does it work?
- Do you use IoT (Internet of Things) devices?
  - If so, how are they used?
- What medium do you use to track patches to your systems?
- Do you develop your own applications?
  - If so, how do you vet what code is used?
- If you develop your own applications, how are you ensuring “DevSecOps” is incorporated?
- What gaps exist in your cybersecurity training programs?
- Do you have an intrusion detection system?
  - How is it configured?
  - Who makes changes when?
- How do you identify what logs need to be watched, who watches them, and how escalation of issues works?
- How are cybersecurity trends watched?
  - Who decides how to react to those trends?
- How long are physical logs retained?
  - Where are they stored?
  - Who has access to them?
- How are physical assets tracked?
  - What happens when they are decommissioned?
  - Are there any physical assets on site that are no longer being used?
- When was your last penetration test?

    - What wasn't tested?
    - Have gaps been fixed?
- Have you run a ransomware or disaster recovery test recently?
    - What were the results?
- When was the last time you had a systems audit or an audit on your controls?
- What happens to the data after the contract ends?
- How are you utilizing the new ISO 27701 Privacy Information Management Systems (PIMS) or National Institute of Standards and Technology (NIST) Privacy 1.0 frameworks?

The NIST Framework for Improving Critical Infrastructure Cybersecurity states:

> "To address privacy implications, organizations may consider how their cybersecurity program might incorporate privacy principles such as:
>
> - Data minimization in the collection, disclosure, and retention of personal information material related to the cybersecurity incident;
> - Use limitations outside of cybersecurity activities on any information collected specifically for cybersecurity activities;
> - Transparency for certain cybersecurity activities;
> - Individual consent and redress for adverse impacts arising from use of personal information in cybersecurity activities;
> - Data quality, integrity, and security; and
> - Accountability and auditing."[9]

Contract with Vendor

Contracts between a government agency and a third-party vendor (contractor or private provider) are a critical tool for effectively managing the resulting records that are created.

Meredith Ward, director of research with the National Association of State Chief Information Officers (NASCIO), recommends some basic precautions that agencies should take in order to reduce cyber-risks in as-a-service IT agreements:

- Perform background verification checks on select high-risk, third party employees.
- Monitor and control third-party access to state systems and data.
- Perform random spot checks of third parties' sites.

[9] National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*. Version 1.1, p. 19. April 16, 2018. Accessed 11/18/2020. https://doi.org/10.6028/NIST.CSWP.04162018.

- Engage an independent third party to assess the third parties' capabilities.[10]

Elements of an Effective Contract

Contracts with third-party vendors should address, at a minimum, the following areas:

- Responsibility for ownership—this needs to be very clear. The standard terms and conditions should state that the records are considered the governmental entity's records and are subject to GRAMA and PRMA. If a vendor requests a variation from the standard terms and conditions, careful thought should be given to whether the variation is to be granted and under what circumstances. If granted, the details must be specified in the contract.

- Contingency plans for unforeseen contract termination or the vendor going out of business—the government agency still owns, and is responsible for, the records unless otherwise stated in the contract.

- Strategies for getting records back from the contractor or private provider in a non-proprietary format.

- Required records management processes.

- Record retention requirements.

- Process for providing appropriate access to records. **Note: it is not legal or ethical for government agencies to negotiate exceptions to GRAMA or PRMA in their contracts with vendors.**

- Privacy requirements.

- Security methods.

- Plans for auditing or monitoring data.

- Consequences for violating the contract.

It is a basic tenet of contract law that one cannot put a condition into the contract that contradicts the law.

Free Assistance Obtaining and Contracting with Vendors

[10] Ropek, Lucas. *Reducing Cyber-risks in As-a-Service IT Agreements,* Government Tech. October/November 2020. Accessed 11/18/2020. https://www.govtech.com/security/Reducing-Cyber-risks-in-As-a-Service-IT-Agreements.html

The Utah Division of Purchasing offers to all public entities in the state of Utah the use of statewide contracts with software service providers that offer thousands of software solutions. If an appropriate product is available, then local governmental entities can purchase it through the State's contractor and won't need to conduct the request for proposal (RFP), negotiate terms and conditions, draft a contract, etc.

The Division of Purchasing also offers education and assistance to local governmental entities to help with creating effective contracts through its courtesy posting program. The Division can help agencies draft the RFP, post it on Utah's Public Procurement Place (U3P, hosted by Jaggaer), coordinate the evaluation process, draft contract documents, and more. Detailed information on the Division's courtesy posting services and the means to get in touch with its team can be found on their website.

Monitor Compliance

A government agency needs to monitor vendor performance and audit data security to ensure that the vendor is complying with terms of contracts and with policies.

Just because your agency writes something into a contract doesn't mean that the vendor will actually follow it. A lot of valuable personally identifiable information passes through the vendors' servers so they have a financial incentive to not delete data that they have agreed to delete.

If your government agency contracts with a third-party vendor, you need to have and follow a plan for dealing with possible non-compliance on the part of the vendor. You should consult with a legal advisor to learn about options and determine the best course of action.

Resources

ISO 27701 Privacy Information Management Systems (PIMS)

National Institute of Standards and Technology (NIST) Privacy Framework 1.0

National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity 1.1

Utah Division of Purchasing and General Services

- Search for established contracts: https://statecontracts.utah.gov/Home/Search
- Video showing how to request a quote on the contract site: https://purchasing.utah.gov/wp-content/uploads/Get_a_Quote.mp4
- List of contracted cloud service providers: https://statecontracts.utah.gov/Home/Search#a3c9Y2xvdWQgc29sdXRpb25zJmNudD1udWxs

- List of contracted Software Value Added Resellers (SVAR): https://statecontracts.utah.gov/Home/Search#a3c9U29mdHdhcmUgVmFsdWUgQWRkZWQgUmVzZWxsZXIgKFN2YXIpJmNudD1udWxs
- Courtesy Posting Services website: https://purchasing.utah.gov/for-agencies/courtesy-posting-services/