Demystifying Data Privacy in the Age of Mobile Identity

How You Can Implement Usher™ with Data Privacy in Mind
Notices

This document contains copyrighted and proprietary information of MicroStrategy Incorporated (including its subsidiaries, “MicroStrategy”). It may be used for internal uses only and may not be copied, distributed, or publicly displayed, in whole or in part, without the express written consent of MicroStrategy. This document is provided for informational purposes only; it is not legal advice and should not be relied on as legal advice. Each customer’s requirements and implementation will vary and MicroStrategy encourages its customers to obtain appropriate advice regarding data privacy laws and other laws applicable to their business prior to any purchase or implementation.

This document is intended to reflect MicroStrategy’s current product offerings and practices and the current state of the laws discussed herein as of the publication date of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of MicroStrategy’s products or services. This document is not warranted to be error-free and does not create any liabilities, warranties, representations, contractual commitments, conditions or assurances from MicroStrategy, its affiliates, suppliers or licensors. The responsibilities and liabilities of MicroStrategy to its customers are controlled by MicroStrategy agreements, and this document is not part of, nor does it modify, any agreement between MicroStrategy and its customers.

The following are either trademarks or registered trademarks of MicroStrategy Incorporated or its affiliates in the United States and certain other countries: MicroStrategy, MicroStrategy Analytics, MicroStrategy Analytics Platform, Usher, MicroStrategy Usher, Usher Badge, Usher Security, Usher Security Server, Usher Mobile, Usher Analytics, Usher Network Manager, and Usher Professional. Other product and company names mentioned herein may be the trademarks of their respective owners.

All Contents Copyright © 2017 MicroStrategy Incorporated. All Rights Reserved.
# TABLE OF CONTENTS

I. Identity Management as a Gateway to Digital Transformation  
II. Privacy Law Landscape in the US and EU  
   - Patchwork Quilt vs. Blanket Law  
   - What Data is Regulated  
   - Processing Personal Data – When is it Lawful?  
   - Cross-Border Transfer of Data  
   - Role of Privacy Notices  
III. Usher Features that Facilitate Compliance with Data Privacy Laws  
   - Provide In-App Privacy Notices to End Users  
   - Tailor Collection of Location Data  
   - Control Usher Data Retention and Obfuscate / Pseudonymize Usher Data  
   - Build Custom Reports in Usher Analytics  
   - Control Access to Usher Data and Network Settings  
   - Rely on MicroStrategy’s Privacy Shield Certification for Data Transfer and Data Security in the Cloud  
IV. Usher in Action – Approaches to Data Privacy Compliance  
   - Use Case #1: Secure Access to Banking Website and Services  
   - Use Case #2: Secure Remote Access to IT Systems  
   - Use Case #3: Drive Customer Loyalty and Gain Actionable Retail Insights  
   - Use Case #4: Issue Time Limited Digital Keys and Secure Vendor Portal  
   - Use Case #5: Drive Recruiting and Increase University Security by Adopting Digital ID Card  
   - Use Case #6: Enable Efficient and Coordinated Emergency Response  
   - Use Case #7: Enhance Delivery Management and Increase Customer Satisfaction  
V. FAQ on Usher and Data Privacy  
VI. Implementation Checklist  
VII. Conclusion / Additional Resources  
VIII. Appendices
Identity management can catalyze your organization’s digital transformation. Many challenges, however, can stand in the way of a successful identity management program. Data privacy concerns are often among them. This white paper provides practical guidance on how you can use MicroStrategy Usher™ as an identity management solution while protecting end user data privacy.

Understanding data privacy principles can be challenging, so this white paper starts with an overview of the data privacy laws in two important markets (the US and EU) that take varying regulatory approaches and describes Usher features that can help facilitate compliance with these regulations. We then review several Usher use cases and discuss how organizations can address data privacy considerations in each case. The white paper concludes by answering some common privacy questions about Usher based on MicroStrategy’s own internal deployment of the product and providing a useful checklist of considerations to assist organizations with their Usher implementations.

I. Identity Management as a Gateway to Digital Transformation

Business is undergoing a digital transformation that is unstoppable. By leveraging data analytics, mobile, cloud, Internet of Things (IoT) and other technologies, organizations are injecting digital power into virtually all business activities. The reasons are compelling: it streamlines processes, enables better decisions, improves customer and employee satisfaction, accelerates the speed of business, and ultimately makes enterprises more profitable. And organizations do it because they have to—the market demands it and their competitors are doing it.

While many factors determine whether an enterprise will succeed in its digital transformation, few are as critical as identity management. Identity management enables activities at the core of the digital transformation for businesses—e.g., using role-based privileges for accessing corporate systems, assigning responsibilities based on identity and managing a distributed workforce on the go, providing highly targeted offers and services to customers, and centralizing enterprise command and control for enhanced personnel safety and asset security. That’s why MicroStrategy developed Usher, a mobile-based enterprise security platform delivering identity management and authentication, logical and physical access controls, and real-time telemetry and analytics.

Success with identity management, however, requires more than a robust technical solution. It also requires addressing the elephant in the room—end user data privacy. In many ways, the digital transformation of business is being helped along by the fact that individuals already have embraced digital practices in their personal lives. From smart phones to online banking to health wearables, people are more immersed than ever in digital life. At the same time, individuals are becoming increasingly aware—and protective—of their personal information, with new laws and regulations reflecting this important concern. Adding to the mix are data privacy laws that can vary widely across countries and be difficult to parse.

This reality presents organizations with the challenge of pursuing digital transformation while protecting end user data privacy. This paper shows how organizations can use Usher to power their digital transformations while crafting data privacy approaches to help ensure business success. Having a basic understanding of the data privacy law landscape is an important first step. So let’s start there, and then we’ll discuss several use cases to illustrate how Usher can be implemented with data privacy in mind.

Understanding data privacy principles can be challenging, so this white paper starts with an overview of the data privacy laws in two important markets (the US and EU) that take varying regulatory approaches and describes Usher features that can help facilitate compliance with these regulations. We then review several Usher use cases and discuss how organizations can address data privacy considerations in each case. The white paper concludes by answering some common privacy questions about Usher based on MicroStrategy’s own internal deployment of the product and providing a useful checklist of considerations to assist organizations with their Usher implementations.
II. Privacy Law Landscape in the US and EU

If you have any working knowledge of data privacy laws, you probably know that there can be many differences in the data privacy laws across different countries. We’ve chosen to focus here on the US and EU because they are currently the world’s largest markets for digital transformation and they reflect two different regulatory approaches to data privacy. In this section, we’ll describe some of the main differences to give you the lay of the land. In addition, we’ll provide important context for our discussion about Usher features that facilitate data privacy compliance and our review of data privacy approaches to Usher implementations. Depending on the nature and location of your business, there may be data privacy laws in other jurisdictions that are relevant. The data privacy laws in many jurisdictions have been inspired to varying degrees by the EU framework, so even if the EU laws don’t apply to your Usher use case, they may still be a helpful lens to use in gauging data privacy considerations.

Patchwork Quilt vs. Blanket Law

THE US RELIES ON A MIXED REGULATORY REGIME…WHILE THE EU HAS A BLANKET DATA PROTECTION LAW

One of the most significant differences between data privacy laws in the US and the EU is that the EU relies primarily on a blanket data protection law that regulates how personal information about individuals can be collected and used, no matter the industry, while the US relies on a patchwork of laws and regulations often targeting specific industries or types of data.

In the US, at the federal level, the most generally applicable law related to data privacy is a consumer protection law known as the Federal Trade Commission Act (FTCA). Section 5 of the FTCA prohibits “unfair or deceptive trade practices in or affecting commerce” and since the late 1990s the Federal Trade Commission (FTC) has used Section 5 to bring numerous privacy actions, including actions alleging that companies failed to protect personal data, changed privacy policies without adequate notice and failed to comply with the terms of a posted privacy policy.

In addition to the FTCA, there are many other federal laws in the US that target specific sectors or types of data. The table below sets out some of the most prominent US federal data privacy laws and the applicable enforcement authority.

<table>
<thead>
<tr>
<th>Industry (Data Type)</th>
<th>Examples of Data Protected</th>
<th>Law</th>
<th>Enforcement Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial (All personal information collected by a financial institution in connection with providing products or services)</td>
<td>Account balances, information submitted for a loan application or payment history</td>
<td>Gramm-Leach-Bliley Act (GLBA)</td>
<td>Consumer Financial Protection Bureau and other federal regulators</td>
</tr>
<tr>
<td>Health Care (Protected Health Information (PHI))</td>
<td>Information about health status, provision of health care or payment for health care</td>
<td>Health Insurance Portability and Accountability Act (HIPAA)</td>
<td>Department of Health and Human Services</td>
</tr>
<tr>
<td>Children (All personal information about a child under the age of 13)</td>
<td>Name, contact information, information about a child’s interests and hobbies and digital information collected through cookies or tracking technologies</td>
<td>Children's Online Privacy Protection Act (COPPA)</td>
<td>Federal Trade Commission</td>
</tr>
<tr>
<td>Financial (Consumer reporting information)</td>
<td>An individual’s credit score or credit report</td>
<td>Federal Consumer Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act (FACTA)</td>
<td>Federal Trade Commission and Consumer Financial Protection Bureau</td>
</tr>
<tr>
<td>Schools (Student education records)</td>
<td>Information regarding student’s performance, credits earned or courses taken</td>
<td>Family Educational Rights and Privacy Act (FERPA)</td>
<td>Department of Education</td>
</tr>
</tbody>
</table>
In addition to these and other federal laws, there also may be US state laws applicable to your business. California tends to lead the way in privacy regulation at the state level, but most states now have enacted some form of privacy legislation. Also, be sure to consider any guidelines issued by applicable industry groups (e.g., the payment card, mobile marketing and online advertising industries). These self-regulatory frameworks can provide guidance on “best practices” in the industry and insight into what customers might expect. In some cases, the self-regulatory frameworks can become compulsory as a result of contractual obligations.

In contrast to the US, the EU relies primarily on a single overarching data privacy framework that applies in all EU member states. Currently the applicable blanket framework that regulates how personal data of individuals can be collected, used, processed and transferred is the EU Data Protection Directive (95/46/EC) (the “EU Directive”). Each EU member state has implemented the EU Directive through its own legislation, which has led to divergent approaches on some data privacy topics and created compliance challenges for many businesses. In 2016, the EU adopted a new overarching data privacy law known as the General Data Protection Regulation (“GDPR”) that will replace the EU Directive and will be directly applicable in all EU member states without the need for implementing legislation. The GDPR does allow EU member states to add enhancements in specified areas, but overall, when it comes into effect in May 2018, the GDPR is expected to increase harmonization of data privacy laws in the EU.

What Data is Regulated

**IN THE EU, PERSONAL DATA IS DEFINED VERY BROADLY AS “ANY INFORMATION RELATING TO AN IDENTIFIED OR IDENTIFIABLE NATURAL PERSON”**

Before we go further, it’s important to understand what kinds of data are regulated by these laws in the US and EU. This question largely turns on the definitions of “personal data” set out in the applicable laws. In the US, there is no single definition of “personal data”. For example, the type of data covered by HIPAA is “protected health information” and GLBA covers certain protected financial information, while the FTCA doesn’t regulate data per se, but prohibits unfair or deceptive acts or practices (which can apply in the privacy context).

In contrast, there’s a single broad definition of “personal data” in the EU, which is “any information relating to an identified or identifiable natural person”. This definition obviously captures identifiers such as a name or national ID number, but also includes other information that could identify a person such as age, physical characteristics, telephone number, address, occupation, IP address, fingerprint, location or some combination of these elements. Let’s look at a few examples for context:

<table>
<thead>
<tr>
<th>Data Examples</th>
<th>Personal Data in the EU?</th>
</tr>
</thead>
<tbody>
<tr>
<td>A name and contact information of an individual at a prospective customer</td>
<td>Yes</td>
</tr>
<tr>
<td>IP addresses of employees or customers</td>
<td>Yes</td>
</tr>
<tr>
<td>A fingerprint</td>
<td>Yes</td>
</tr>
<tr>
<td>Records about employee work hours</td>
<td>Yes</td>
</tr>
<tr>
<td>A resume</td>
<td>Yes</td>
</tr>
<tr>
<td>Aggregated data about consumer ages</td>
<td>No</td>
</tr>
<tr>
<td>A list of customer birthdates (without names associated)</td>
<td>No</td>
</tr>
</tbody>
</table>

In short, the EU data privacy framework defines personal data extremely broadly, while in the US, the type of information regulated varies depending on the industry or data type being targeted by the applicable law (e.g., financial information, health information, education records, etc.).

**Processing Personal Data – When is it Lawful?**

Now that we’re familiar with the concept of personal data, let’s turn to what “processing” means because it’s a term used frequently in EU data privacy parlance. This term comes from the EU Directive and the GDPR and essentially means anything that is done to, or with, personal data (including collecting, recording, storing, transmitting, sharing, using or deleting data). The US federal laws regulating data privacy don’t use this “processing” concept. Under the EU Directive and the GDPR, personal data of individuals can only be processed if one of the following conditions is met (these are known as “processing conditions” or “lawful bases”):
### Processing Conditions in the EU

<table>
<thead>
<tr>
<th>Processing Condition / Lawful Basis</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consent</td>
<td>The individual has given consent to the processing of his/her data</td>
</tr>
<tr>
<td>Performance of a Contract</td>
<td>The processing is necessary for the performance of a contract with the individual or to take steps at the request of the individual prior to entering into a contract</td>
</tr>
<tr>
<td>Legal Obligation</td>
<td>The processing is necessary for compliance with a legal obligation under the EU or member state law</td>
</tr>
<tr>
<td>Vital Interests</td>
<td>The processing is necessary to protect the vital interests of the individual or another person</td>
</tr>
<tr>
<td>Public Interest or Exercise of Official Authority</td>
<td>The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority</td>
</tr>
<tr>
<td>Legitimate Interests</td>
<td>The processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the individual)</td>
</tr>
</tbody>
</table>

### Applying Processing Conditions in the Real World

<table>
<thead>
<tr>
<th>Processing Activity Example</th>
<th>Possible Processing Condition / Lawful Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td>An operator of a mobile application that provides a mapping and navigation service (e.g., Google Maps or Waze) collects user location to provide route suggestions and directions.</td>
<td>Consent. When the individual downloaded the mobile application, the operator provides a privacy notice describing the information collected and how it’s used. Prior to downloading the application, the user accepted the privacy notice and consented to the processing.</td>
</tr>
<tr>
<td>An online vendor collects a buyer’s delivery address and credit card billing address when the buyer purchases goods online.</td>
<td>Performance of a Contract. The vendor needs the buyer’s address to deliver the goods purchased and the vendor needs to collect the buyer’s billing address to verify the buyer’s payment information.</td>
</tr>
<tr>
<td>An employer collects tax information (e.g., national ID, number of dependents, etc.) from employees for payroll purposes.</td>
<td>Legal Obligation. This processing is necessary for compliance with EU or member state laws regarding taxation.</td>
</tr>
<tr>
<td>A healthcare provider collects medical information about an individual in connection with providing emergency medical services.</td>
<td>Vital Interests. This processing is necessary to protect the vital interests of the individual.</td>
</tr>
<tr>
<td>An employer processes salary information and bank account details from employees to pay their salaries.</td>
<td>Performance of a Contract. The employer needs this information to effect payment pursuant to an employment agreement.</td>
</tr>
<tr>
<td>A professional association processes member information to maintain a member roster and process disciplinary procedures.</td>
<td>Exercise of Official Authority. The professional association has official authority to process information of its members in this manner.</td>
</tr>
<tr>
<td>A local government runs a library and collects patron’s names and check-out/in history in connection with running the library service.</td>
<td>Public Interest. Collecting names and check-out/in history is necessary to run the library (a task in the public interest).</td>
</tr>
<tr>
<td>A company provides law enforcement personal data regarding an employee in connection with a criminal investigation.</td>
<td>Public Interest. Providing this data is necessary for investigation of a crime (a task in the public interest).</td>
</tr>
</tbody>
</table>

You may be wondering how data processing activities fit into these categories and, in particular, how you can use data collected by Usher given these restrictions. Below we’ll go through some data processing examples and assign a possible “processing condition” so you can see how these conditions can apply to (and allow for) common data processing activities. Then we’ll take a more in-depth look at the legitimate interests processing condition and apply the balancing test required by that processing condition to a few examples. We imagine that many companies seeking to deploy Usher will either be relying on the consent or legitimate interests processing conditions to collect and use Usher data, however, other processing conditions could apply as well. In Section IV, we’ll review specific Usher use cases to see some examples of how processing conditions could apply to Usher, but first, let’s get familiar with the concept of processing conditions in general.

The legitimate interest processing condition is the least straightforward of the processing conditions available under EU law and reliance on this condition requires consideration of two questions. First, is the interest “legitimate”? And second, does the “legitimate interest” outweigh the individual’s interest in privacy? The EU data
protection authorities have issued specific guidance on both of these questions. They recognize that a broad range of interests can be legitimate – from trivial, to somewhat important, to very compelling interests. The basic guidelines from the EU data protection authorities state that to be legitimate, an interest must be: lawful, clearly articulated, and represent a real and present interest (i.e., not be merely speculative). An opinion issued by EU data protection authorities, cites the following (among others) as examples of legitimate interests:

- Exercise of right to freedom of expression or information
- Direct marketing
- Unsolicited non-commercial messages (e.g., charitable or political in nature)
- Enforcement of legal claims
- Prevention of fraud
- Employee monitoring for safety or management purposes
- Physical, IT and network security
- Historical, scientific or statistical purposes

Once you establish that an interest is legitimate, you then need to weigh that interest against the individual’s interest in privacy with respect to the data proposed to be processed. In performing this balancing test, the EU data protection authorities recommend considering the following factors:

- Is the processing necessary for the legitimate interest being pursued (i.e., are less invasive methods available to achieve the same interest)?

- What is the volume of data being processed and how broadly is the data being made accessible?
- What are the reasonable expectations of the individual in the privacy of the data?
- What safeguards have been applied to prevent undue impact on the individual?

Where the legitimate interest is compelling and the privacy interest is low, the company is likely to meet the balancing test. Alternatively, where the legitimate interest is not very important and the privacy interest is high, the company is not likely to meet the balancing test. As you might expect, in many cases the outcome of the balancing test will not be clear and a detailed analysis will be required to determine whether the legitimate interest hurdle is met. See an illustration of this balancing test in Appendix 1.

Now let’s go through some examples where a company might seek to rely on the “legitimate interest” processing condition and apply the EU guidance to determine if the interest is legitimate and if the balancing test is satisfied. Note that we are just using short summaries of example fact patterns here and applying these tests in the real world would require a detailed review of the facts and circumstances, as well as any applicable regulatory guidance.

<table>
<thead>
<tr>
<th>Fact Pattern</th>
<th>Summary</th>
<th>Legitimate Interest Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>A company uses a debt collection agency to seek repayment of a debt and discloses the debtor’s name and last known address to the collection agency.</td>
<td>Company Interest: Compelling&lt;br&gt;Individual Interest: Low&lt;br&gt;Outcome: Satisfies Test</td>
<td>Legitimate Interest: The Company has a legitimate interest in collecting on a debt. Balancing Test: This processing is necessary for a legitimate interest and only the information necessary is provided to the debt collection agency. Although the individual may have an interest in keeping the information private, he does not have a reasonable expectation of privacy with respect to this data.</td>
</tr>
<tr>
<td>A store collects contact details from customers at the time of a sale and uses this contact information for future product marketing by mail and email. Customers are informed about the opportunity to object (and in this case the customer has not objected).</td>
<td>Store Interest: Medium Importance&lt;br&gt;Individual Interest: Low&lt;br&gt;Outcome: Satisfies Test</td>
<td>Legitimate Interest: The store has a legitimate interest in marketing its products. Balancing Test: This processing is necessary for a legitimate interest and only the customer’s contact details are being used. Although the customer has an interest in the privacy of his contact information, it’s reasonable for him to expect he will receive offers as a customer of the store and he has not exercised his right to object.</td>
</tr>
<tr>
<td>An employer deploys an MDM solution to employees as part of a BYOD program and elects to collect information regarding all mobile apps on the employees’ devices to make sure certain apps that pose a security risk are not installed.</td>
<td>Employer Interest: Compelling&lt;br&gt;Employee Interest: High&lt;br&gt;Outcome: Likely does not satisfy test</td>
<td>Legitimate Interest: The employer has a legitimate interest in IT and data security. Balancing Test: Collecting all applications on an individual’s mobile device is a significant intrusion and is not necessary for achieving the interest (the employer can instead set up the MDM to flag certain high risk apps). The employee has a high interest in privacy with respect to his mobile applications which could reveal sensitive information about the employee.</td>
</tr>
</tbody>
</table>
Unlike the EU, the US privacy regime is largely disclosure oriented – as long as notice is provided to the individual, the privacy laws generally don't impose substantive limits on how personal data can be used or require the presence of a particular condition prior to processing personal data.

In addition to needing a “lawful basis” to process data, data processing activities in the EU must meet the following other basic requirements:

1. Data must be processed lawfully, fairly and in a transparent manner;
2. Data must be accurate and, as necessary, kept up to date;
3. Data must be deleted or anonymized when it’s no longer needed for the purpose it was originally collected;
4. Data collection and processing must be limited to what’s required to satisfy the original purpose;
5. Data must be processed in a manner that ensures appropriate security and protection against unlawful processing and loss, destruction or damage;
6. Data must be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with the original purpose; and
7. Under the GDPR, the data controller will also be required to demonstrate that its data processing activities comply with items 1 – 6 above.

In the US, there's no similar list of basic data processing requirements, however, the Federal Trade Commission does take enforcement action against companies that use data in ways that are incompatible with the purpose stated in the applicable privacy notice, so requirement #6 above is similar in the US framework. In addition, although there's more flexibility around data retention in the US, in general, data should only be kept as long as reasonably necessary, which is similar to requirement #3 above.

**Cross-Border Transfer of Data**

Restriction on cross-border data transfers is one of the clearest areas of divergence between the data privacy laws in the US and EU. US privacy laws generally don't impose restrictions on the transfer of data outside the US, while the EU laws on data transfers outside the EU are very strict. In the EU, it's unlawful to transfer personal data of individuals to countries that the EU has determined don't have “adequate” data protection laws (this includes the US) unless the individual has consented to the transfer or the transferor has adopted certain protections most commonly evidenced through binding corporate rules, model clauses or the Privacy Shield framework. Since obtaining the consent of the individual is not practical in most scenarios, most companies that transfer more than minimal data from the EU to the US would rely on one of the other transfer mechanisms. Keep in mind that “transfer” is defined broadly and includes actions such as viewing a report in the US that includes personal data stored in the EU.

**Role of Privacy Notices**

In the US, for companies not otherwise subject to industry specific regulations (such as HIPAA and GLBA) or data specific regulations (such as COPPA and FERPA), there's no federal law that requires provision of a privacy notice prior to collecting personal data. However, several states have laws that require notice to the individual when an organization collects personal information in the online and mobile contexts. California’s Online Privacy Protection Act is the most prominent such law, and it applies to the personal information of California residents regardless of where the website or mobile application operator is located – in practice, California’s law (and similar other state laws) requires all website and mobile application operators to provide a privacy notice.

In the EU, all companies must provide a privacy notice before collecting an individual’s personal data regardless of the industry or method of data collection (online or otherwise). The GDPR has expanded the amount of information required to be included in privacy notices and, somewhat paradoxically, also now specifically requires those notices to be concise and in plain English. The table in Appendix 2 sets forth the basic requirements for a privacy notice in California and in the EU.

In the website and mobile app contexts, both the US and the EU require a privacy notice to end users (in accordance with the varying requirements set out in Appendix 2), but the role of the privacy notice varies significantly. In the US, if you’re not operating in a regulated industry or gathering data that’s specifically regulated, as long as you provide a clear and accurate privacy notice that meets the applicable state law requirements and then use the data
accordingly, you're almost certainly going to meet the compliance requirements of US law. In the EU, on the other hand, regardless of your industry and method of collecting data, the privacy notice itself is only one of the affirmative compliance requirements.

Before we move on to discussing the Usher features that can help you comply with data privacy laws, let's review some the main differences between data privacy laws in the US and EU that we've discussed.

<table>
<thead>
<tr>
<th>Topic</th>
<th>US</th>
<th>EU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overarching Data Privacy Law</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Definition of Personal Data</td>
<td>Varies depending on the underlying law</td>
<td>Broadly defined as any information relating to an identified or identifiable natural person.</td>
</tr>
<tr>
<td>Data Processing Must Be Legitimized on Specific Grounds</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Privacy Notice Required Prior to Data Collection</td>
<td>Not at the federal level outside of certain regulated industries and types of data. Some states require a privacy notice prior to collection of data online or through a mobile application.</td>
<td>Yes</td>
</tr>
<tr>
<td>Cross-Border Transfer of Data Restricted</td>
<td>Not regulated at the federal level. Certain states have laws that limit state agencies from outsourcing data processing outside the US.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**III. Usher Features that Facilitate Compliance with Data Privacy Laws**

Now that you know some of the basics about data privacy laws in the US and EU, it's easy to see how some of the data collected by Usher can be considered “personal data” under the EU privacy framework and that several US regulations may be relevant to your Usher implementation such as state privacy notice requirements and the FTCA. As you begin an Usher implementation, you may start getting questions about data privacy from either internal constituents or end users. We've thought a lot about these questions in our own use of Usher and have designed Usher to help you to comply with data privacy laws applicable to your business. Now let’s go through some of the Usher features that can facilitate compliance with data privacy laws.

**Provide In-App Privacy Notices to End Users**

As discussed earlier, providing privacy notices to individuals before collecting any personal data is a required step for compliance in the EU and is also required in the US for collecting data online or through mobile apps. In addition to satisfying a legal requirement, privacy notices are an important opportunity for you to communicate directly with your end users and provide information to help them understand how their personal information is processed in connection with Usher.

During the Usher badge set-up process, an administrator has the opportunity to provide a privacy notice to the end user. The privacy notice will be accessible to the end user at any time in the Usher badge, and for jurisdictions where consent (as opposed to just notice) is required from the end user prior to collecting data, the administrator can require the end user to review the privacy notice and check “accept” before downloading the Usher badge. If your Usher network has multiple badges, you can have a separate privacy notice for each badge as needed to address varying legal requirements or uses of data.

If you need to update your privacy notice due to changes in your Usher implementation (e.g., adding physical or logical access or expanding your use to include Bluetooth beacons), changes in data use, or changes in legal requirements, the administrator can easily replace the in-badge privacy notice with a new one and can require a fresh “consent” or include a pop-up notification that the privacy notice has changed, depending on the requirements in the jurisdiction.

**Tailor Collection of Location Data**

As discussed earlier, in the EU personal data can only be collected if a “lawful basis” exists for the collection. Location data is not treated differently than personal data generally, but the EU data protection authorities do take the view that individuals have a heightened interest in privacy with respect to location data, so this sensitivity should be taken into account when considering the basic requirements for data processing in the EU such as processing data fairly and transparently, collecting the minimum amount of data.
necessary and only using data for specified and explicit purposes. In addition, if a company processing location data is relying on “legitimate interests” as its processing condition, it should make sure the “legitimate interest” is sufficiently compelling to meet the balancing test (discussed in more detail in Section II).

Administrators of an Usher network have several options when it comes to how much location data to collect. If an administrator sets up an Usher badge so that location is not required, then no location data will be collected unless an end user chooses to allow the Usher application to access location data (access wouldn’t be required for the Usher badge to work). If an administrator wants to collect location data, there’s an option to collect location data when an end user takes an action with an Usher badge or to collect location data each time the end user’s location changes (in both cases, the Usher badge won’t work if the device settings don’t allow access to location data). Administrators should consider the type of Usher implementation planned, the expected end users (e.g., employees, customers, etc.), the nature of the business and the applicable privacy laws when determining appropriate location settings for the Usher network.

Also, keep in mind that regardless of the location settings selected by the administrator, end users always have control over the location-sharing settings on their mobile devices. The end user may not be able to access their Usher badge if the required location settings are not in place, but they still do maintain ultimate control over when Usher can access their location data. You can draw a parallel to popular map mobile applications such as Waze or Google Maps – the end user can always decide to turn off the app’s access to location when the map is not in use and re-authorize access as needed.

In addition to collecting location data from mobile devices, Usher can also gain location-awareness of end users through interaction with Bluetooth-enabled beacons. Where an Usher implementation includes the use of beacons, the administrator has flexibility to deploy beacons as broadly as desired depending on the applicable data privacy laws and planned uses for such data. For example, in the US, a broad deployment of beacons might be acceptable as long as end users are appropriately notified, while in the EU where data privacy laws are stricter, use of beacons may need to be narrower in some circumstances.

**Control Usher Data Retention and Obfuscate / Pseudonymize Usher Data**

As discussed earlier, two basic principles of EU data protection law include that (i) only the minimum amount of data necessary to achieve the business purpose should be collected and (ii) data should only be kept as long as necessary for the original purpose it was collected. We ship Usher with MySQL, an open-source relational database management system, which an Usher administrator can use to set up a script to delete Usher data on a set schedule of their choosing based on the type of Usher implementation, the applicable data privacy laws and planned uses of the Usher data. For example, if a company is using Usher to control employees’ physical access to its facilities, it may determine that it only needs to keep access records for a few weeks because the planned use of the data is to identify and address security incidents (which may be known relatively quickly). On the other hand, if a company is using Usher to evaluate use of its conference room space to assist with facilities planning decisions, it may want to keep the data longer because it would be relevant to see conference room utilization over several months to make a long-term decision regarding facilities planning.

There also may be instances where an administrator would like to obfuscate or pseudonymize certain personal data, rather than deleting it entirely. For example, in the prior example where Usher is being used to assess conference room utilization for facilities planning, the company may not need to know end user names if they are viewing conference room data on an aggregate basis (e.g., conference room 10 has an 80% utilization rate). To meet the EU requirement of only collecting the minimum amount of data needed for the stated purpose, an administrator may want to obfuscate or pseudonymize end user names so that they are not available as a reporting metric in Usher Analytics. This Usher data would still be available in the Usher server logs, but it would not be available for reporting in Usher Analytics.

**Build Custom Reports in Usher Analytics**

For many Usher implementations, we envision organizations will want to use Usher data for a variety of purposes and an administrator may not want to delete or remove data as laid out in the previous examples. Usher also allows administrators to filter reports in Usher
Analytics so that only information necessary for the purposes of a specific report is included. Take an example of a retailer that has deployed Usher to its customers in a loyalty application and also uses Bluetooth beacons in their stores. One purpose of the beacon data may be to see where customers spend time in the store on an aggregate basis (e.g., 200 people were in the men’s department between 2 and 4 pm). Another purpose of the beacon data may be to send a specific customer a coupon based on buying history, location or other factors. For the first purpose, user names aren’t necessary because the company is viewing data in the aggregate, but for the second purpose, end user name are necessary to target coupons to specific individuals. An administrator can filter each report in Usher Analytics so that the minimum amount of data necessary is being processed in each instance.

Another reporting feature that isn’t strictly necessary for compliance purposes, but could be useful for providing transparency and strengthening the trust of end users is providing end users access to self-service dashboards containing their own Usher data. If you're interested in making a self-service dashboard available to your end users, our services professionals can help you get started with a standard dashboard template. Many employers enable a similar feature for their mobile device management solutions to increase transparency with employees.

**Control Access to Usher Data and Network Settings**

The EU requirement that processing personal data should be appropriately limited is known as the “data minimization principle”. In addition to requiring a company to limit collection of data to only data necessary to achieve the purpose, it also requires companies to limit data access to individuals that need the data for the stated purpose. So, for example, if your HR department collects employee bank account information to pay employees, access to that data should be limited to people who need it to perform payroll activities (e.g., senior managers in HR and the payroll team).

Usher has a roles-based system to allow you to manage access to Usher data and limit who can make changes to your Usher networks settings. The table below sets out the various administrator roles in Usher and the privileges associated with each role. As you can see, only people that are designated as Usher Analysts will have access to Usher data.

<table>
<thead>
<tr>
<th>Role</th>
<th>What They Can Do</th>
<th>Can View Usher Data?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usher Administrator</td>
<td>Create new Usher networks, create new Usher badges, configure Usher network</td>
<td>NO</td>
</tr>
<tr>
<td></td>
<td>(e.g., to add logical or physical gateways), modify Usher network and badge settings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Send badges to new members of a network, revoke badges from users in a network</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Designate Usher Analysts, Usher Professional Users, Helpdesk Users</td>
<td></td>
</tr>
<tr>
<td>Usher Analyst</td>
<td>View all Usher data and run analytics reports</td>
<td>YES</td>
</tr>
<tr>
<td>Helpdesk User</td>
<td>Read-only access to view Usher network settings, view user account (what badges they have, when they received, revoked badge)</td>
<td>NO</td>
</tr>
</tbody>
</table>

**Summary of Role-Based Access to Usher Data**
The individuals you designate as Usher Analysts will depend on the type of Usher implementation you have and the planned uses of Usher data. For example, if you’re using Usher to control physical access to your office space, you may only need your Facilities department or other risk management personnel to be designated as Usher Analysts. In contrast, if you’re using Usher as an ID card for your customer loyalty program, you may want various sales and marketing executives to be designated as Usher Analysts. Regardless of whom you designate as an Usher Analyst, you’ll want to inform them about use restrictions and you can track what reports are run in Usher Analytics to confirm compliance with internal policies, including any relevant privacy notices. Usher provides the flexibility to minimize data access and leaves an audit trail for compliance review.

Rely on MicroStrategy’s Privacy Shield Certification for Data Transfer and Data Security in the Cloud

If your Usher implementation will involve end users in the EU and you’re planning to use Usher Analytics in the US, or otherwise transfer Usher data from the EU to the US or another jurisdiction that has not been deemed by the EU to have “adequate” data protections in place, you’ll need to consider what data transfer mechanism you’re going to rely upon to transfer Usher data. If you’re planning on a Cloud implementation of Usher using MicroStrategy’s Cloud or a virtual private cloud MicroStrategy has set up for you in AWS, then you’ll be able to rely on Privacy Shield as the mechanism for transferring data from the EU to MicroStrategy Cloud because MicroStrategy has self-certified to the EU-US Privacy Shield framework. In addition, you should investigate what data transfer mechanisms your company is currently relying on to transfer employee and business data from the EU to the US to determine if your Usher data is within the scope of those existing arrangements. You have the option to encrypt all data stored in MicroStrategy Cloud.

Scans barcode while buying lunch at cafeteria for loyalty points
Validates identity over phone with helpdesk using Usher code
Accesses garage lift-gate, elevator, and office floor using beacon sensing
Uses two-factor to VPN into business system from home
Attends workout class; attendance automatically logged via beacons for fitness competition
Uses web SSO to switch between web-based applications and log progress on team projects
Logs off work computer via Bluetooth proximity
Scans QR code to validate parking and leave for the day
IV. Usher in Action – Approaches to Data Privacy Compliance

Now let's look at some specific Usher use cases to see how Usher can be used to solve common business challenges in a variety of industries and discuss how you can approach data privacy compliance in each scenario.

Use Case #1:
Secure Access to Banking Website and Services

Business Challenge: A global bank wants to differentiate its customer experience and reduce fraudulent transactions without placing unnecessary demands on users or sacrificing convenience.

Usher Solution: The Bank can deploy an Usher badge (in the form of a digital banking card) to its customers. Customers can use the Usher badge to securely access the Bank's website or ATM machines using multi-factor authentication, time-limited access codes or QR codes. The Bank also can verify a customer's identity for customer service or phone transactions using one-time passcodes as opposed to security questions, which often be easily guessed or otherwise discovered.

Possible Data Privacy Compliance Approach: The Bank can use the Usher application to provide its end users (customers in this case) with a privacy notice that meets the applicable legal requirements and use the Usher data in accordance with this notice. In the EU, where a “processing condition” is necessary to lawfully collect or use data (see Section II), the Bank could rely on consent of the end user. As part of the Usher badge download process, the Bank can require certain users (e.g., users in the EU) to review and click “accept” to the privacy notice prior to downloading the Usher badge. For US users, the Bank can just make the privacy notice accessible within the Usher badge instead of requiring an active “accept” from the end user. The Bank should also consider the basic data processing requirements of EU law such as deleting or pseudonymizing data when no longer necessary, adequately securing data and minimizing access to data (see Section II).

You can find more information on Usher solutions for the banking industry here.

Use Case #2:
Secure Remote Access to IT Systems

Business Challenge: With a global salesforce constantly on the move and an increased number of employees opting for flexible work arrangements, including teleworking, a software company needs to provide an easy and secure way for employees to access critical IT assets remotely. The Company’s current system for remote access, which relies on physical tokens that are frequently lost or misplaced, hinders productivity and increases security risks.

Usher Solution: The Company can integrate Usher with its VPN solution and issue Usher badges to its employees. The Company can configure Usher to replace or augment passwords for VPN access. With Usher, remote workers can log into VPNs using Usher security codes, push notifications, QR code scans and/or biometrics. Usher comes with built-in integration for popular VPN systems including Cisco, PulseSecure, PaloAlto, FS, Citrix and others.

Possible Data Privacy Compliance Approach: The Company can use the Usher application to provide its end users (employees in this case) with a privacy notice that meets the applicable legal requirements and use the Usher data in accordance with this notice. In the EU, where a “processing condition” is necessary to lawfully collect or use data (See Section II), the Company may determine not to rely on consent as its processing condition because the EU takes a skeptical view of consent where there’s a power imbalance between the person requesting consent and the person providing consent (i.e., in the employer-employee context). In this case, the Company
may instead be able to rely on the “legitimate interest” processing condition. This condition is the least clear-cut of the available processing conditions under EU law and requires a balancing of the Company’s interests in processing data against the individual’s interest in data privacy. Here, where the Company has a strong interest in protecting its critical IT systems, the Company should be in a good position to demonstrate that it meets the “legitimate interests” test. The Company should also consider the basic data processing requirements of EU law such as deleting or pseudonymizing data when no longer necessary, adequately securing data and minimizing access to data (see Section II).

You can find more information on logical access capabilities of Usher here.

Use Case #3: Drive Customer Loyalty and Gain Actionable Retail Insights

**Business Challenge:** A global retailer’s business is becoming increasingly digital and retailer wants to develop a consistent, personalized and frictionless digital customer experience to drive revenue. In addition, to fuel its data-driven marketing and sales efforts, the Retailer needs a unified view of each customer’s identity and touchpoints with the Retailer, whether through online or in-store purchases, interactions with customer service or logging into a store website.

**The Solution:** The Retailer can leverage the Usher SDK to build a store mobile application and issue digital loyalty cards to its customers (in the form of an Usher badge). Customers can present the badge for in-store purchases to receive “reward points”, validate their identity over the phone with customer service representatives and login the store website without a password. In addition, the Retailer plans to deploy beacons in its stores and to send location-based coupons to customers and offer other customized VIP-shopping experiences. The Retailer can build dashboards using Usher Analytics to gain real-time insight into customer activities from anywhere.

**Possible Data Privacy Compliance Approach:** The Retailer can use the Usher application to provide its customers with a privacy notice that meets the applicable legal requirements and use the Usher data in accordance with this notice. If the Retailer has end users in the EU such that the requirement for a valid processing condition applies, the Retailer may be able to rely on consent as the processing condition because its end users are customers. As part of the Usher badge download process, the Retailer can require users to review and click “accept” to the privacy notice prior to downloading the Usher badge. The Retailer should also consider the basic data processing requirements of EU law such as deleting or pseudonymizing data when no longer necessary, adequately securing data and minimizing access to data (see Section II).

You can find more information on Usher solutions for the retail industry here and more information on Usher Analytics here.

Use Case #4: Issue Time Limited Digital Keys and Secure Vendor Portal

**Business Challenge:** A large US restaurant chain wants to create a secure vendor portal to place orders and pay vendors. Once an order is placed, the Restaurant needs the ability to provide the vendors with time-limited access to its facilities to make food and supply deliveries. When a delivery is in process, the Restaurant would like to know the location of the vendor to estimate delivery time.

**Usher Solution:** The Restaurant can secure its vendor portal using Usher and can issue digital Usher badges to its vendors and Restaurant managers. Restaurant vendors and managers can login to the portal using only Usher (with no password) or Usher can serve as a second factor of authentication in addition to a password. Once the Restaurant
places an order in the portal, the Restaurant can issue a time-limited Usher key to the vendor to access the Restaurant’s facilities to make the delivery. The Restaurant can set up the Usher network to enable location tracking on the Usher badge so that Restaurant can gain insight into vendor location when a delivery is in process.

**Possible Data Privacy Compliance Approach:** The Restaurant is operating in the US, so the primary laws to consider are state laws (such as California) that require providing a privacy notice prior to collecting personal information in the online and mobile contexts. Although there is no general requirement to get an active consent in the US, some states have laws that prohibit electronic tracking of individuals without consent, so we’d recommend that the Restaurant to set up Usher to require a consent during the badge download process since they are planning on collecting precise location data. Once the privacy notice is issued, the Restaurant can use the Usher data in accordance with this notice and delete the data once it is no longer necessary.

You can find more information about the logical and physical access capabilities of Usher here and here and you can learn more about location capabilities of Usher here.

**Use Case #5:**

**Drive Recruiting and Increase University Security by Adopting Digital ID Card**

Business Challenge: A US University believes that current methods of campus identity verification, such as physical ID badges or passwords, are simply not safe enough. Physical University IDs can easily be forged, lost, or stolen and passwords are frequently forgotten or written down by students. The University also needs a solution for providing visitors and alumni limited access to certain University facilities at set times. The University is looking to add security to their current identity management architecture and drive recruiting and donation initiatives by embracing a digital solution.

**Usher Solution:** The University can issue digital ID cards (in the form of an Usher badge) to students, faculty and administrators to provide customized access to University facilities (laboratories, athletic facilities and faculty areas) and IT systems. The University can issue temporary digital Usher badges to visitors and alumni that provide access to only designated areas during a visit or event. The University security staff can use Usher Analytics to gain insight into typical user behavior to spot abnormal activities. In an emergency, University administrators can send campus alerts to Usher badge holders via their devices.

**Possible Data Privacy Compliance Approach:** The University can use the Usher application to provide students with a privacy notice and use the data in accordance with this notice. There also is a federal data privacy regulation related to educational records (known as FERPA) that the University should consider. An “educational record” is any record that contains information directly related to a student which is maintained by an educational agency or institution. FERPA gives students (or parents when students are under age 18) the right to access and seek to amend educational records and in some cases the right to control disclosure of personal data from the educational records. Although Usher data (e.g., physical and logical access records) may fit within the definition of “educational record”, we expect that most Usher data would not be kept long enough to make it the subject of many FERPA requests. In addition, we believe the primary target of FERPA is educational records related to credits earned and performance records, which are likely to be of more concern and interest to students and their parents than Usher data.

You can find more information about Usher solutions for higher education here and more information about Usher Analytics here.
Use Case #6:
Enable Efficient and Coordinated Emergency Response

**Business Challenge:** The City of New York needs a way to quickly dispatch police, fire, EMS and other first responders in emergency situations and to enable first responders across various agencies and regions to verify each other’s identity and coordinate. Currently when first responders arrive on the scene from multiple agencies, they don’t have a way to easily verify one another’s identity without relying on physical ID badges, which can be easily counterfeited, damaged or lost. In addition, people managing emergency response don’t have a way to communicate with an intra-agency response team and easily disseminate information, for example to notify the group about a dangerous condition or get assistance to a specific individual. The City would also like a way to quickly send a “status check” survey to determine if members of a response team are safe.

**Usher Solution:** The City can issue an Usher badge to first responders across agencies. Each first responder’s Usher badge can include his or her name, agency, rank and any relevant special credentials (HAZMAT, SWAT, etc.). When an emergency arises, necessary personnel can be dispatched to an emergency using the Usher Professional app, based on their location and other credentials. First responders that arrive on the scene can validate one another using time-sensitive, single use codes or can scan the QR code on another’s badge. An emergency response manager could see the location of the response team and communicate to the group or a specific first responder. The response manager could also send a survey to the response team (which first responders can quickly respond to by checking a box “yes” or “no”) to determine if first responders on the ground are safe or require assistance.

**Possible Data Privacy Compliance Approach:** The City can use the Usher application to provide first responders with a privacy notice. Based on several FTC enforcement actions and influential federal and state guidance documents, we’d recommend that the City set up Usher to require a consent during the badge download process since they are planning on collecting precise location data. Once the privacy notice is issued, the City can use the Usher data in accordance with the notice and delete the data once it’s no longer necessary.

You can find more information about Usher solutions for government and emergency response [here](#).

Use Case #7:
Enhance Delivery Management and Increase Customer Satisfaction

**Business Challenge:** A US-based food delivery service has a mobile application that allows customers to place food orders from local restaurants for delivery. The Service provides customers with an estimate of their food delivery time, but often there are circumstances at the restaurant or otherwise that lead to delay. The Service needs a way to allow customers to see the location of their food delivery in real time, which would reduce costs associated with staffing customer service lines to handle customer inquiries. The Service would also like a way to verify the delivery time of each order to track on-time delivery rates.

**Usher Solution:** The Service can leverage the Usher SDK to include Usher functionality in its existing mobile application and can issue an Usher badge to its customers and drivers. Customers could use Usher to login to the Services' website or mobile app and the Service could build a custom dashboard to allow customers to see the location of their delivery in real time, which would reduce costs associated with staffing customer service lines to handle customer inquiries. The Service would also like a way to verify the delivery time of each order to track on-time delivery rates.

**Possible Data Privacy Compliance Approach:** The City can use the Usher application to provide first responders with a privacy notice.
Possible Data Privacy Compliance Approach: The Company is operating in the US, so the primary laws to consider are state laws (such as California) that require providing a privacy notice prior to collecting personal information in the online and mobile contexts. The Company can provide a “Driver Badge” to its drivers and a “Customer Badge” to its customers and can use Usher to provide a badge-specific privacy notice to each group of individuals. For drivers, location tracking would be enabled on the Driver Badge to funnel this data to the customer-facing dashboard. Based on several FTC enforcement actions and influential federal and state guidance documents, we’d recommend that the Company set up Usher to require a consent during the badge download process because precise location data will be collected. Once the privacy notices are issued, the Company can use the Usher data in accordance with these notices and delete the data once it’s no longer necessary.

You can learn more about location capabilities of Usher and integration with beacons here.

V. FAQ on Usher and Data Privacy

Now that we’ve gone through some concrete Usher use cases, you’re probably seeing some common themes in terms of how you can implement Usher with privacy in mind: issue a privacy notice, follow the privacy notice, ensure you have a valid processing condition in the EU, delete Usher data when you no longer need it and keep in mind the other basic processing requirements applicable in the EU. We hope it’s becoming clear how Usher can help solve common business challenges and how its features can help you to set up and use Usher in a manner that complies with data privacy laws. The Q&A section below covers some additional topics we encountered in our own use of Usher that you may find helpful:

Q: If an Usher implementation will involve end users in many different countries, is a different privacy notice needed in each country?

A: Not necessarily—but this depends on the location of the end users and your organization’s preferences. For our internal deployment of Usher across MicroStrategy’s worldwide employee base, we’ve taken the approach of providing one privacy notice applicable to our US employees and a separate privacy notice that meets the requirements of EU data protection laws, which is applicable to all our non-US employees. This approach means that we’re probably providing a more robust privacy notice than is legally required in some non-US jurisdictions, but we felt that this was a good trade-off to reduce the administrative burden of maintaining a different privacy notice in each non-US jurisdiction specifically tailored to the applicable laws.

Q: Can I set up an Usher badge to collect data related to an end user’s location when an Usher transaction takes place?

A: In the US, as long as the end users are appropriately notified, it’s acceptable to collect location data at the time an Usher transaction takes place (i.e., accessing a door or logical system).

In the EU, a company must have a lawful basis for collecting data (see Section II). If the end users in your Usher implementation are customers, vendors, partners or other non-employees, you can consider consent as your processing condition. If the end users in your Usher implementation are your employees, the EU data protection authorities often don’t recognize consent as a valid processing condition, so you may need to rely on the “legitimate interests” processing condition. Determining whether this processing condition is satisfied requires a balancing of your company’s interest in collecting the data against the individual’s interest in privacy with respect to the data (see Section II for more information). Where location data is being collected, the employee’s interest in privacy will be relatively high, so you’ll need to make sure your organization’s interest is sufficiently compelling (e.g., IT security).

Q: Can I set up an Usher badge to collect location data each time an end user’s location changes?

A: For starters, we wouldn’t recommend that you set up your Usher badge to collect every significant location change of your end users unless you have a business need for this data. Although there’s no specific US federal or state law regulating GPS data, the FTC has brought several enforcement actions in the geolocation context and California and the Mobile Marketing Association have each published influential guidance documents on the topic. As a result, if you do have a business need for this data, we’d recommend you explain that data processing clearly in your privacy notice and require your end users to click “accept” to the privacy notice during the Usher badge download process.

In the EU, you need a valid processing condition to collect this data. Where your end users aren’t employees, you can consider consent
as your processing. However, if your end users are employees you may need to rely on the “legitimate interests” processing condition, which may be challenging given that employees have a strong interest in the privacy of their location data. Some instances where an employer’s legitimate interest could outweigh an employee’s interest in this type of location data include businesses where knowing employee location is essential for the company to do business (such as a package delivery business or taxi-service) or if knowing employee location is critical to the employee’s safety (such as a mining company). See Section II for more examples of the legitimate interest balancing test.

Q: Are there restrictions on how a company can use the Usher data?
A: In the US, as long as the Company’s uses are consistent with its privacy notice, data privacy laws generally don’t restrict what the Company can do with Usher data. Keep in mind however, that other non-data privacy laws could apply – for example, you could not use Usher to track employee location and then take an employment action against all employees that attended church on Sunday.

In the EU, if your lawful basis for collecting the data is consent, then, as long as you're acting according to your privacy notice and meet the other basic processing conditions stated in Section II, your use is likely acceptable. However, if your lawful basis for collecting the data is the “legitimate interests” of the Company, you’ll need to weigh the legitimate interests of the Company in processing the personal data against the individual’s interest in privacy to determine if the use is lawful. See Section II for more detail on this balancing test.

Q: How can a company manage use of Usher data so that it’s consistent with the privacy notice?
A: As discussed earlier, access to Usher data can be limited to individuals designated as Usher Analysts. We’d recommend providing these individuals with guidelines specifying the acceptable uses of the Usher data (as set out in your privacy notice). You can also track reports that are run in Usher Analytics to make sure stated policies are being followed.

Q: Since the Usher application comes with a privacy notice, can companies deploying Usher just use that instead of developing their own privacy notice?
A: Although the Usher application comes with a privacy notice, each enterprise deploying Usher should create their own privacy notice to provide to its end users in the Usher badge. These notices can vary broadly depending on how enterprises are implementing Usher and the policy that comes with the Usher app is most likely not specific enough for your use to meet legal requirements. In the US, a privacy notice is not legally required in all jurisdictions, but we think it’s good practice to provide one and increases transparency with end users. Creating your own privacy notice is pretty straightforward. It should set forth the basic details about your use of Usher – what data you are collecting, how you are using it, who you are sharing it with, etc. See Appendix II for an overview of requirements for privacy notices in California and the EU.

Q: Does MicroStrategy have access to my Usher data?
A: If you have an on-premise implementation of Usher or an implementation in your own virtual private cloud, MicroStrategy can’t access your Usher data. If you have a Cloud implementation either in MicroStrategy Cloud or in a virtual private cloud MicroStrategy has set up for you in AWS but you have your data warehouse on-premise or in your own virtual private cloud, MicroStrategy can’t access your Usher data. Even if you store your data warehouse in the MicroStrategy Cloud or in a virtual private cloud MicroStrategy has set up for you in AWS, it’s MicroStrategy’s policy not to access customer data unless requested by the customer for technical support purposes or if otherwise required by law. You also always have the option to encrypt your data in a Cloud implementation. Note that we never sell your Usher data to third party advertisers or spammers.
VI. Implementation Checklist

As you’ve surely noticed, consideration of the data privacy laws relevant to your Usher implementation depends on how you’re using Usher and who your end users are and where they’re located. So, before you begin developing your approach to data privacy, we’d recommend you gather some basic information on the Usher use being planned from key stakeholders. Below is a high-level checklist of preliminary considerations to use as a guide:

<table>
<thead>
<tr>
<th>Preliminary Topics to Consider</th>
</tr>
</thead>
<tbody>
<tr>
<td>What kind of Usher implementation are you considering (physical access, logical access, Usher Professional reporting, Bluetooth beacons etc.)?</td>
</tr>
<tr>
<td>How does your organization plan to use Usher data? Will there be different uses in different jurisdictions?</td>
</tr>
<tr>
<td>Who are your planned end users (employees, customers, suppliers, vendors etc.)?</td>
</tr>
<tr>
<td>Where are your planned end users located?</td>
</tr>
<tr>
<td>Who will the primary users of Usher Analytics and Usher Professional be (facilities, IT, managers, Sales, etc.)?</td>
</tr>
<tr>
<td>Will your organization be hosting Usher on premise or using MicroStrategy Cloud?</td>
</tr>
</tbody>
</table>

Once you have a good handle on the questions above, below are the basic data privacy topics we’d recommend considering with input from your legal department or Chief Privacy Officer:

<table>
<thead>
<tr>
<th>Data Privacy Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine which privacy laws are relevant for your planned Usher implementation.</td>
</tr>
<tr>
<td>Draft privacy notices to provide to end users.</td>
</tr>
<tr>
<td>Discuss implementation with other constituencies as necessary (works councils, unions, Data Privacy Officers).</td>
</tr>
<tr>
<td>Develop / update other internal policies if necessary (e.g., employee handbook, employment agreements, contractor/services agreements, policies regarding Usher data access and use).</td>
</tr>
<tr>
<td>Determine whether you’ll be transferring data outside of the EU (e.g., to the US) and the transfer mechanism you’ll rely on (Privacy Shield, model clauses, binding corporate rules, etc.).</td>
</tr>
<tr>
<td>Develop end user communications regarding the Usher implementation.</td>
</tr>
<tr>
<td>Educate those with access to Usher data regarding appropriate uses.</td>
</tr>
<tr>
<td>Educate HR (for employee deployments) or Customer Service (for customer deployments) on common Usher questions they may receive from end users.</td>
</tr>
</tbody>
</table>

VII. Conclusion / Additional Resources

A robust identity management platform with features that facilitate data privacy compliance can power an organization’s digital transformation. As this white paper shows, Usher meets these requirements by providing a mobile-centric user experience for interacting with business processes and applications across an enterprise and using an architecture built with data privacy in mind. Designed for flexibility and ease of use, Usher can be deployed across a wide range of organization types – from retailers to financial institutions to higher education. Leveraging the MicroStrategy Analytics Platform, Usher also enables a full range of analytics reporting on your Usher network so you can gain valuable and actionable business insights.

Next Steps with Usher

- START A TRIAL
- GET MORE INFORMATION

About MicroStrategy Incorporated

Founded in 1989, MicroStrategy (Nasdaq: MSTR) is a leading worldwide provider of enterprise software platforms. The Company’s mission is to provide customers with a world-class software platform and expert services so they can deploy unique intelligence applications. To learn more, visit MicroStrategy online, and follow us on Facebook and Twitter.

References

1. Examples include: 1) age at which a child can provide valid consent online (range is 13 – 16 years old), 2) appointment of data protection officers, 3) introduction of further restrictions on the processing of employee data, 4) ability to pass laws to limit rights in areas such as national security, crime and judicial proceedings, and 5) amendment to reconcile data protection with freedom of information, to protect information subject to professional secrecy and restrict processing of national identity numbers.


3. The first two fact patterns come directly from Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC published by the Article 29 Working Party and adopted on April 9, 2014. This opinion includes many more examples of legitimate interest balancing test and is a good resource for more information.

4. The EU has deemed the following countries adequate from a data protection perspective: Andorra, Argentina, Australia, Canada, Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, and Uruguay.

5. The EU-US Privacy Shield is a framework that provides a mechanism for companies to transfer data from the EU to the US in compliance with EU restrictions on cross-border transfers. Companies certifying to the Privacy Shield must adhere to certain privacy and security principles to help ensure that personal information collected in the EU is appropriately protected in accordance with the Privacy Shield principles when sent to the US.
APPENDICES
Appendix 1 | Illustration of Legitimate Interest Balancing Test Under EU Law

<table>
<thead>
<tr>
<th>Company's legitimate interest</th>
<th>Individual interest in privacy and data protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMPELLING</td>
<td>LOW</td>
</tr>
<tr>
<td>Likely to meet balancing test</td>
<td>Detailed analysis required</td>
</tr>
</tbody>
</table>
Appendix 2 | Overview of Privacy Notice Requirements

The table below sets out a summary of the requirements for privacy notices under California law and under EU law (pursuant to the GDPR). As discussed in Section II, in the US, the California’s Online Privacy Protection Act is the most prominent US state law that specifies requirements for a privacy notice.

<table>
<thead>
<tr>
<th>California</th>
<th>EU (GDPR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Describe personal information collected</td>
<td>Describe personal information collected</td>
</tr>
<tr>
<td>Identify third-parties with whom personal information will be shared</td>
<td>Identify third-parties with whom personal information will be shared and state whether data will be transferred to another country</td>
</tr>
<tr>
<td>Explain process for an individual to review and make changes to his personal information collected (if allowed by the website or mobile app operator)</td>
<td>Inform individual of the following rights:</td>
</tr>
<tr>
<td>Explain how individual will be notified of changes to a privacy policy</td>
<td>Right to request access to and correction or erasure of personal information</td>
</tr>
<tr>
<td>State the effective date of the privacy policy</td>
<td>Right to object to processing</td>
</tr>
<tr>
<td>Disclose how the operator responds to web browser “do not track” signals or other mechanisms that provide consumers the ability to exercise choice regarding collection of data about online activities over time and across third party web sites, if applicable</td>
<td>Right to data portability</td>
</tr>
<tr>
<td>Disclose whether other parties may collect personally identifiable information about an individual’s online activities over time and across different websites when an individual uses the operator’s site or service</td>
<td>Right to withdraw consent at any time, if applicable</td>
</tr>
<tr>
<td>Disclose whether other parties may collect personally identifiable information about an individual’s online activities over time and across different websites when an individual uses the operator’s site or service</td>
<td>Right to make complaint with a supervisory authority</td>
</tr>
<tr>
<td>State that if further processing will occur for a purpose other than set out in the notice, additional information will be provided to the individual</td>
<td>Describe the purposes of the data processing and the applicable legal basis (including the legitimate interest pursued if applicable)</td>
</tr>
<tr>
<td>State the period for which the personal information will be stored, or if not possible, the criteria used to determine that period</td>
<td>State that if further processing will occur for a purpose other than set out in the notice, additional information will be provided to the individual</td>
</tr>
<tr>
<td>State the identity and the contact details of the “data controller” and any data protection officer</td>
<td>State the identity and the contact details of the “data controller” and any data protection officer</td>
</tr>
</tbody>
</table>