M+E JOURNAL

Today's localization challenges are enormous. The opportunities are unprecedented. Is the industry ready for the mayhem?

GIVING VOICE TO CHAOS

SECURITY SOLUTIONS
The threats to our most valuable assets are many. M+E vendors are on top of it.

WORKFLOWS AND THE CLOUD
Much has changed in the way we track, access, move and store everything we deal with.

SMART CONTENT
The many ways the industry adopts new technologies to make content smarter.

22.02

IDENTIFYING INTERNATIONAL DATA PRIVACY RISKS IN LOCALIZATION OPERATIONS

Today’s privacy challenges call for standardized industry controls and benchmarks

ABSTRACT: Localization workflows include processing high volumes of freelancer personal data (translators, adaptors, subtitlers, etc.) by the supply chain. The data is often subject to extra-territorial data protection and entire supply chains are co-responsible for each other’s compliance. Data is shared, without monitoring, by all stakeholders. Shorter project turn-arounds make it difficult to verify and monitor resource/vendor compliance. Industry best practices haven’t integrated data protection particularities of localization workflows. Service providers and their clients need global understanding to mitigate risks.

By Nicole Quilfen, Chief Operating Officer, Mediartis, and
Stephanie Iyayi, Senior Vice President, Legal, Privacy, Convergent Risks

In today’s increasingly digital and global age, many companies in the media and entertainment sector have embraced a critical strategy for capturing new markets worldwide: content localization. So, why are localization workflows the industry’s modern Trojan Horse? For the simple fact that freelancer personal data and partner compliance are frequently neglected in data privacy strategies.

Since the European General Data Protection Regulation (GDPR) came into effect in 2018, many organizations have been performing privacy and security gap analysis assessments and investing in data security and privacy tools. Privacy policies have been adapted to secure the personally identifiable information of customers and in-house personnel. Vendor privacy assessments are increasingly popular, often carried out as part of a due diligence process, in large part due to the regulation's notion of compliance co-responsibility. However, while the industry has made significant progress, the processing of freelancers' personal data in production workflows and the lack of standardized vendor privacy controls leave companies exposed to data breaches as these data are often overlooked in privacy strategies and unaddressed in policies.

> *COMPANIES NEED COMPLIANCE visibility across their global resources, the controls to meet the requirements of global, regional, and country compliance regulations and simplified partner compliance visibility to mitigate non-conformity risks.*

HIGH RISK AREAS: FREELANCER PERSONAL DATA AND PARTNER COMPLIANCE

Production workflows are particularly high risk as they involve processing high volumes of freelancers' personal data. Service providers have long considered the size of their talent database as a key business asset but are now considering the resources in a different light when the data relates to European citizens or residents.

Freelance contracting has become the norm in localization. During pre-production, all project stakeholders work together and share high volumes of freelancer personal data during a very concentrated period to agree on the best resources for a project: voice actors, translators, subtitlers, QA analysts, post editors, etc. Unsecured and unmonitored, personal data circulates extensively between internal services and production and dubbing companies, studios, agents, creative directors, and content owners. Resources are untracked and original data sources and privacy compliance are often unknown.

Data is shared physically via email, uploaded to FTP addresses and clouds, etc., with no visibility of how the data is being processed on the receiving end where shared data is often added to internal databases for future projects, thus exposing the data controller to data breaches. Further complicating data protection management, these databases are often maintained by individual services as talent contracting tends to be managed directly by the related service, and the data remains under the radar of data protection controllers and the data compliance is left unmanaged.

Compiled over time, these databases often contain outdated data, whose original source and compliance status are unknown. In fact, data subjects are often unaware their data is being processed and shared with third parties — regularly transferred across borders, and rarely secured or encrypted. Companies processing this personal data have specific legal obligations to respect, even if the data was collected before the legislation came into effect, and failure to do so can result in penalties of up to €20 million or four percent of their last fiscal year's global revenue, litigation from a high-profile individual or damage to a company's reputation, should a breach arise.

WORLDWIDE DATA PRIVACY

The GDPR represented a landmark for data protection. Trading blocs, governments, and privacy organizations took note, and over the last four years, the regulation has inspired new data privacy legislation worldwide. Regulations like the European legislation are driven locally within Europe, but the scope of impact is global and applies to the processing of European residents' data, no matter where in the world the data processing takes place. Any business, no matter where they are located, that uses, processes, or controls data for European citizens and residents must meet all the requirements of the regulation. This responsibility flows from any entity processing data and the data controllers that provide that direction.

In its most simple terms, the legislation defines personal

__Stephanie Iyayi__ is the senior vice president of legal and privacy for Convergent Risks. She comes from a legal background specializing in privacy and data protection and advises clients on all areas of UK and EU data protection law, from general privacy compliance to risk management issues, compliance implementation, privacy impact assessments, data breach incidents, cross-border data transfers, employee monitoring and data subject access requests.
info@convergentrisks.com @ConvergentRisks

__Nicole Quilfen__ is the chief operating officer of Mediartis. She comes from a business development background specializing in international strategy, personal data protection, and accompanying media and entertainment localization partners with their operational privacy strategies.
*nicole@mediartis.com @Mediartis_*

data as any information that can be used to identify an individual such as names, addresses, emails, telephone and social security numbers, etc., and provides specific guidelines for processing what is referred to as "special categories of data" such as data revealing racial or ethnic origin, religious beliefs, or biometric data like the voice which, in almost all circumstances, infers an individual's identity. Voice data is particularly unique, given that a vocal recording may reveal, inter alia, the ethnic origin of an individual (through accent) or a potential health condition such as Parkinson's which can affect speech. Sensitive personal data such as the voice, is subject to even more stringent protections under the regulation and must be encrypted in transit and at rest.

OUTSOURCING AND PARTNER NON-COMPLIANCE RISKS

Security guidelines, detailed in industry best practices, provide standardized benchmarks that simplify vendor selection and monitoring. Vendor privacy controls, however, have not yet been integrated into the industry's playbook, and without a roadmap or standards for evaluating compliance, vendor selection is risky, complicated, and next to impossible for organizations to monitor without third-party verification. Project-specific partner privacy assessments are crucial for content providers, creators, and owners for vendor selection and monitoring, and for service providers when subcontracting local projects.

Frequent outsourcing of projects by multilanguage vendors to single language vendors in each target country, who sometimes outsource externally themselves, multiplies data breach risks as project compliance is difficult to verify when tier two and three vendors contribute to projects. Supply chain compliance is critical because the European privacy regulation introduces the notion of co-responsibility, meaning that a data breach at any step puts companies at risk of administrative fines. While most regulatory action has been focused on controllers, the Commission National de l'Informatique et des Libertés, a GDPR supervisory authority, fined both a data controller and its data processor for breach of security in January 2021 because they failed to comply with their respective obligations.

PRIVACY COMPLIANCE — WHERE TO BEGIN?

In short, all resources need to be compliant and workflows involving the storage or exchange of personal data should be adapted to comply with the European regulation and adapted for local and regional-specific legislations.

Data controllers must ensure that data on European residents is only exported to places with similar data protection rules, keeping in mind that if the shared data is biometric, additional security measures probably apply. Canada, Brazil, Japan, New Zealand and South Korea and many other countries have adopted measures modelled on the European regulation. While there is currently no data privacy law applicable to all industries in the United States on the federal level, every state has their own data privacy laws for example, California's privacy regulation overlaps with the European legislation in many areas.

Compliance documentation requirements are extensive, and some include keeping privacy notices, policies, operating procedures, data processing records, risk assessments, third party data processing agreements, government submissions, various consent forms, etc., which must be in line with local regulations. Procedures respecting data retention and processing should also be reviewed and updated to meet regulations, and personal data must be deleted where there is no longer a legitimate need for processing it. Companies should document and record all of this if any supervisory authority investigates a complaint or logged event.

Freelancer consent of processing must be 100 percent independent of any work contract, recorded and up to date. If the data is sensitive or biometric, explicit opt-in consent should be renewed every two years. Organizational processes and the infrastructures supporting them, human and technology, must be adapted to support data protection legal obligations. Even sharing or using the data between internal services can be risky if secure compliance policies and framework are not in place.

Successful internal compliance begins with third-party data protection impact assessments across all services. Audit and Gap analysis provide clarity on areas an organization needs to focus on. Organization-wide training and awareness is imperative for compliance success and regular privacy health checks will make sure your strategy is effective. Data breach plans should be as solid as security breach plans and ready for immediate deployment.

Organizations must ensure technical and operational processes are in place to ensure data subjects' rights can be met, for example, right to be forgotten, data portability, the right to object and subject access requests, including access to voice recordings. Privacy compliance should be integrated into internal audit processes, identifying all cross-border data flows, reviewing data export mechanisms, developing, and rolling out training across all personnel to ensure an adequate understanding of data protection principles, responsibilities and internal and external risks.

In summary, the localization industry has complex challenges to meet which are driven by various global compliance regulations. Service providers and their clients face many different scenarios as each country they do business in may have different requirements for data privacy and protection. Today's privacy challenges call for standardized industry controls and benchmarks. Companies need compliance visibility across their global resources, the controls to meet the requirements of global, regional, and country compliance regulations and simplified partner compliance visibility to mitigate non-conformity risks. ⊞