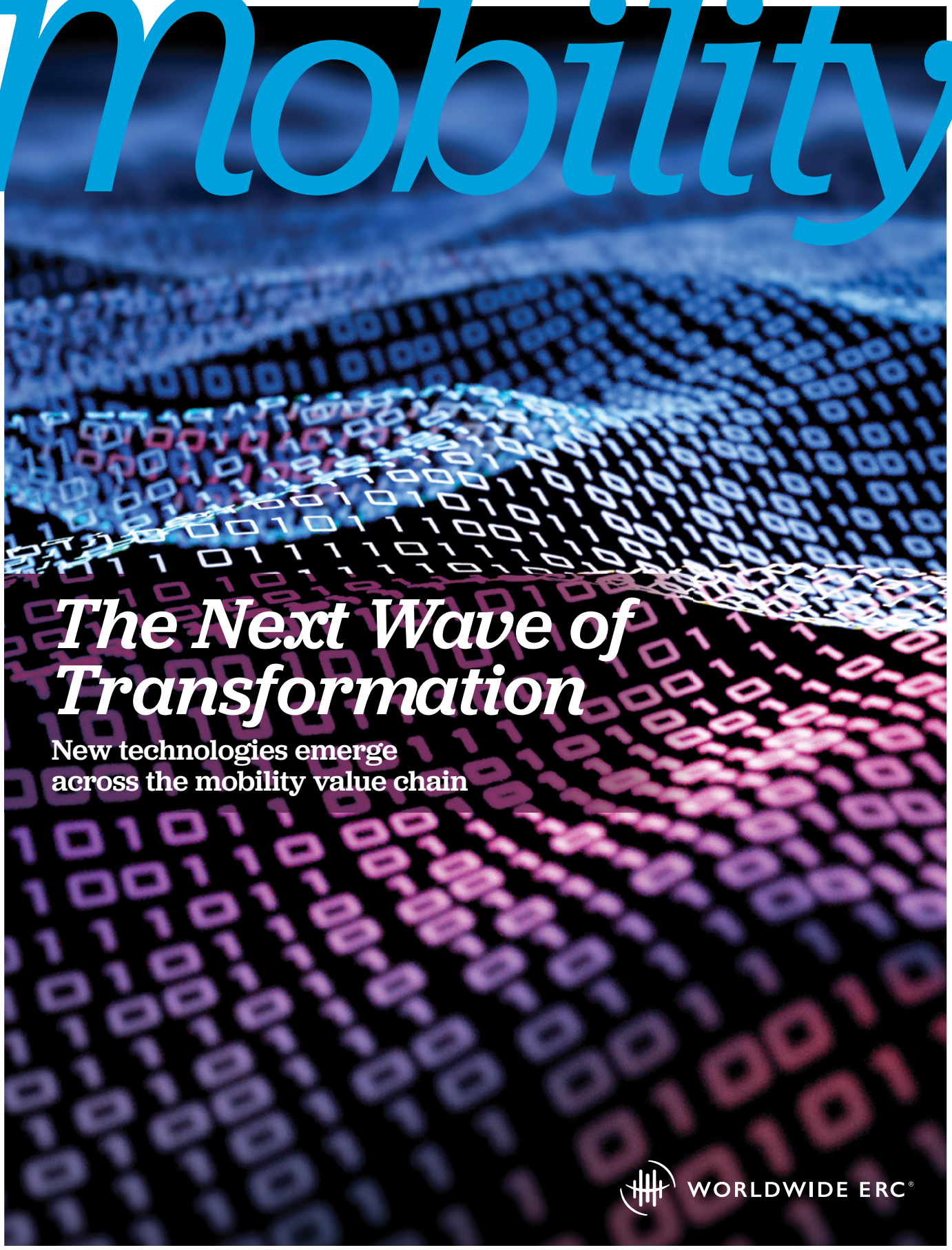
Issue 4 2022

Mobility™



The Next Wave of Transformation

New technologies emerge across the mobility value chain

WORLDWIDE ERC®

worldwideerc.org

New Ways for International One-Way Transfers
THIS POLICY APPROACH CAN SAVE COSTS AND GIVE EMPLOYEES FLEXIBILITY

Strategies for the Remote-ification of Work
ATTRACT NEW TALENT AND SPUR COMPANY GROWTH

Care in Crisis
COMPANIES ARE REDEFINING TODAY'S DUTY OF CARE FOR OVERSEAS WORKERS

New Approaches to Data Privacy

BY TRISTAN NORTH

As the mobility industry continues to rely on technology to provide new capabilities and time-saving efficiencies, the security and protection of data that fuels many of these advances becomes increasingly important.

Few are more qualified to talk about these issues than George Powdar, chair of Worldwide ERC® Public Policy's Compliance Forum. Powdar is senior vice president of global reporting and compliance for relocation management firm Altair Global and has spent more than 35 years in the mobility industry.

TN: How is the global workforce mobility industry dealing with the myriad data privacy and protection standards in the U.S. and around the world?

GP: Data privacy protection laws and requirements are some of the top issues impacting the industry. While the data we collect, store, and share is critical for the services that relocation managers provide to their clients, the process for protecting this information is not always straightforward.

Since the European Union introduced the General Data Protection Regulation (GDPR), which went into effect in 2018, we have seen several countries, as well as many states within the U.S., pass or discuss data privacy laws, which is a big step in the right direction. In the U.S., we have four states that have now passed laws, and a bipartisan group in Congress is discussing the implementation of data privacy laws at the federal level.

But around the world—including in Europe—we have also seen many changes or enhancements to data privacy laws. So even though we've had the GDPR since 2018 and 27 countries have signed on to those data privacy laws, we continue to see specific exemptions or interpretations regarding some of the regulations.

As such, the lack of a unifying standard means that not only must we keep up with these changing requirements, but that the structures we have established to meet these requirements must be continuously updated and monitored.

TN: Are organizations adapting one set of internal policies that adhere to all the different privacy standards? Or, are they taking different approaches depending on the requirements governing a particular set of data?

GP: The GDPR basically sets the framework for how data privacy laws should be managed and what those privacy requirements should be. For the most part, other countries—and here in the U.S., states like California and Virginia—are using a similar framework. That's a good thing.

On the other hand, the guidelines don't incorporate all the different standards. So, ensuring compliance requires an ongoing review of these new laws, as well as continual monitoring, which can be difficult.

TN: To your knowledge, are there provisions of different data privacy laws that contradict one another? For example, what about the length of time you can retain someone's data?

GP: Yes, there are differences. At Altair, we comply with those data retention requirements at the client level. In the U.S., for example, we have a seven-year data retention requirement, which is driven primarily by tax laws. In Europe, that requirement can vary by country. So, to ensure that we at Altair comply with the various data retention requirements, they're set within our agreements with our clients.

In addition, we have had to address the customer's rights within privacy laws. As an example, within the GDPR and in California, the customer has the right to determine how long we keep their data and can request companies to delete their information at any time. Therefore, to ensure compliance, we establish policies and procedures within client agreements to make sure this issue is addressed.

> So, now it's not only a requirement on an RMC that they can protect a customer's information, but we are also required to make sure the suppliers we use, especially the smaller ones, can meet the data protection requirements.

TN: In June of this year, a bipartisan group of U.S. Congressional committee leaders unveiled a federal data privacy standard for the U.S. If enacted, what are the key provisions that you believe need to be included?

GP: There is obviously a considerable amount of interest in a national data privacy standard that would supersede state requirements. I think such a law would make it easier for companies, including the relocation management companies, to comply. That's the model Europe has already adopted. With GDPR being four years in practice, I think most organizations have policies and procedures to comply. If the U.S. law can model what GDPR does, even though many of the states are already doing similar things, I think that would be a big benefit.

Clearly, the law should also address customer rights the way the GDPR does, where customers would have rights in terms of an organization's use of their information. I would also like to see some form of threshold placed on the size and types of companies required to comply. A large percentage of Worldwide ERC's membership, especially on the supplier side, is made up of smaller organizations. Requiring small organizations to abide by these regulations will place a financial strain on companies

that might not have the financial resources to meet all those requirements.

TN: The Worldwide ERC Compliance Forum, which you chair, has been leading the way on protecting the personally identifiable information of transferees who are shipping their household goods to the U.S. Do you see other areas of particular concern when it comes to data privacy and relocation?

GP: One of the things that we see today—and it's also happening right now in Europe—is an increased focus on the transferring and/or sharing of customer information to other countries. As a supplier or a relocation management company, we collect a tremendous amount of information from our customers and their families, and we have to demonstrate that we can securely store that information within our organization. But when you must share that information with other third-party suppliers, either within the country or cross-border, there is an increased risk. So, now it's not only a requirement on an RMC that they can protect a customer's information, but we are also required to make sure the suppliers we use, especially the smaller ones, can meet the data protection requirements. From an organization's perspective, that puts a tremendous burden on RMCs, because now we're basically responsible for ensuring that whoever we use can meet these contractual requirements.

TN: What other areas in your forum deal with technology's impact on mobility?

GP: From a technology perspective, obviously data protection is a major issue for us because many of our organizations have had to invest in technology that showed we could comply with the data privacy regulations. Now, we find that we are responsible not only for using the latest technology for storing and maintaining the accuracy of the data, but we have to ensure that we're adopting the latest and most effective technologies to defend against things like hacking and the increase in cybertheft.

In addition, organizations are focusing a lot of attention on compliance reporting, whether it is built around data security; human rights; capital resources; or environmental, social, and governance factors. All contain different regulations or policies that have to be met or followed, and each adds a layer of complexity to the reporting structure. *m*

Tristan North is the government affairs adviser for Worldwide ERC®. He can be reached at +1 703 842 3400.