Always Designing for People®

Guide to **safeguarding payroll data** in internationally expanding organisations

Faced with an increasingly professionalised cybercrime industry and a more dispersed global workforce, tackling security vulnerabilities needs to be one of the top concerns of every company's agenda.

In our experience, enterprise-level executives need to focus on both data privacy and data security aspects of payroll data protection. This makes sense when you consider the legislative push in this area over recent years, with the introduction of high-profile (and high-penalty) laws like the European Union's General Data Protection Regulation (GDPR) and China's Personal Information Protection Law (PIPL).

Delivering equal data protection across all your geographies

We surveyed over 1,700 senior payroll leaders of international companies and asked what contingency measures they had in place to protect their payroll operations in the event of cyber-attacks or critical systems outages. Only 52% said they have developed a playbook and a contingency plan across all of their geographies. 36% said they'd developed playbooks and plans for some of their countries, while 13% had no plans in place at all.[1]

Merely going through the motions without an effective plan when it comes to safeguarding employees' pay-related information in all of your countries — whether existing territories or new target markets — is simply too big a risk to take. It's also a compliance imperative, considering that there are both stand-alone cybersecurity laws and cybersecurity aspects of existing privacy laws already in place.

The good news is, expansion presents an opportunity to take stock, carry out cybersecurity hygiene and identify where your payroll data could potentially be misused or made vulnerable to bad actors.

It can be tempting to dive in with the technical aspects of information security. In this guide, we'll talk you through the aspects to consider around the organisational, technical and physical components of your payroll data security.

Payroll data security: the organisational considerations

Although there are universal measures you can take to protect payroll information security in a global operating environment, the relative risk you face will also depend on:

- The countries you operate in (and access to/level of local expertise)
- The model of the payroll technology you use (on-premise/cloud-based/outsourced)
- How your global payroll function is organised (centralised or otherwise)

38%

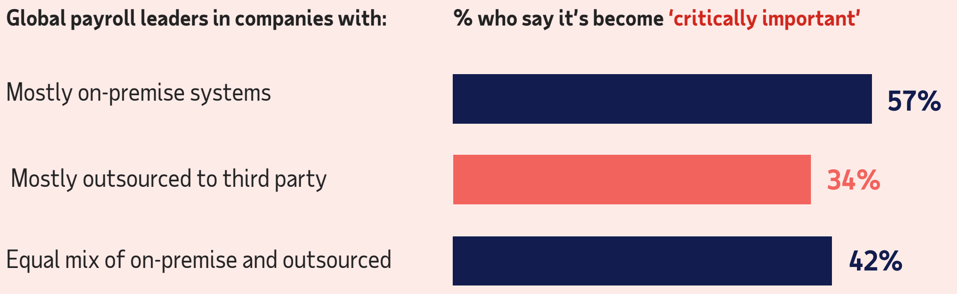
of payroll leaders say they plan to **improve their global payroll data security** as a worldwide initiative over the next 2-3 years, with similar percentages planning the same at regional and in-country level.[1]

The influence of your payroll technology model

Over the last decade there had been a trend for organisations to run payroll in-house (the number of firms doing so jumped from 28% in 2013 to 45% in 2019[4]). Since 2019, there's been a rethink, and more companies are now opting to contract out payroll management to third-party providers, like ADP.

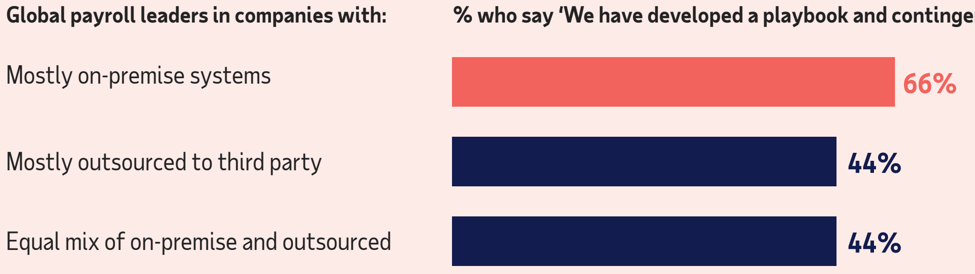
According to our recent study, companies who outsource their payroll completely seem less concerned about the relative importance of data security within their payroll strategy, and less likely to feel the need to make backup plans across all their countries:

To what extent has data security in your payroll strategy become 'critically important' over the last 12 months?



Companies who mostly outsource their payroll seem significantly less concerned about data security than those running payroll mostly on-premise

Considering the increase of cyber-attacks and critical systems outages, what contingency measures do you have in place to protect your payroll operations?



34% of global firms who run payroll in house have no Plan B if security fails in any one country

Findings from ADP report: The potential of payroll in 2024: Global payroll survey

The influence of your payroll organisational model

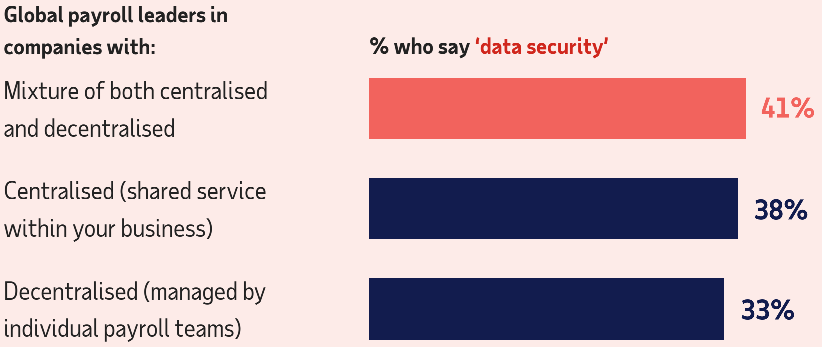
Is your payroll function set up to handle the security challenges of expansion?

Global companies whose payroll is run by individual teams or vendors around the world are less likely to say they plan to focus on data security over the next few years than those with centralised teams or a mixed approach.

If a payroll team is centralised, and managing payroll for all or most business units, it's more likely to have overall responsibility for mission-critical aspects such as data protection and business resiliency. When individual teams (or vendors) around the world run payroll for respective in-country or regional territories, however, central oversight and accountability are much harder to achieve.

Payroll leaders in decentralised teams may lack access to the skills, resources and budgetary commitment to prioritise these all-important security aspects.

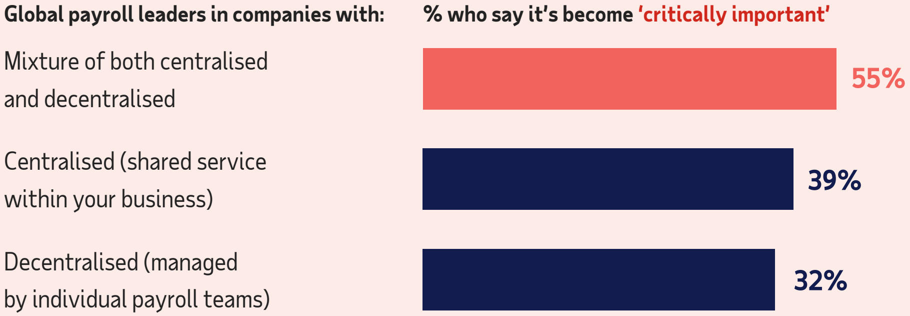
Over the next 2-3 years, what aspects of your worldwide payroll do you plan to improve upon?



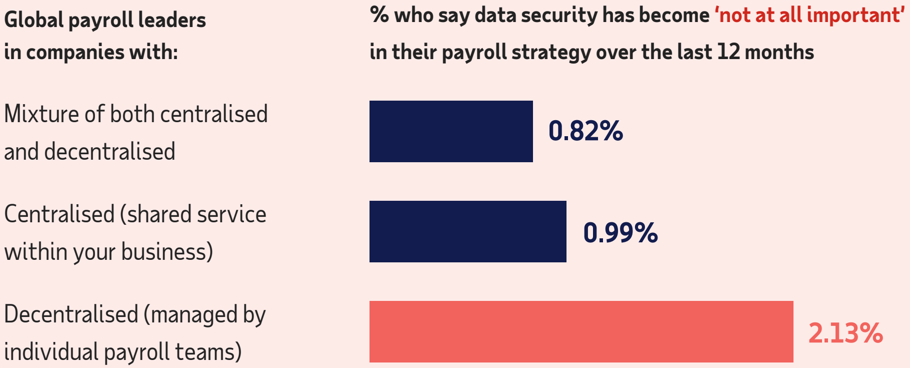
Findings from ADP report: The potential of payroll in 2024: Global payroll survey

Global firms with decentralised payroll teams are a lot less likely to rank data security as a critically important component of their payroll strategy.

To what extent has data security in your payroll strategy become important over the last 12 months?



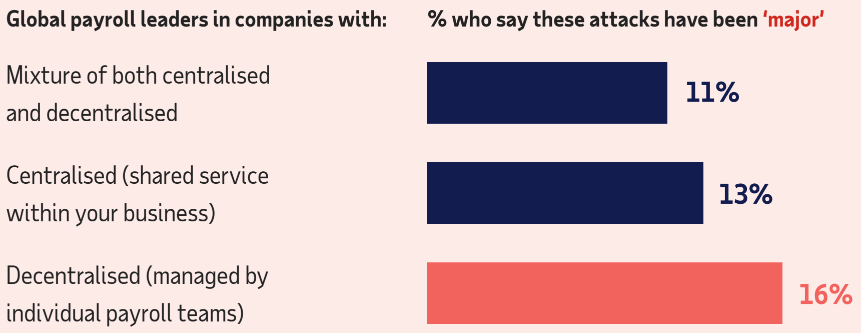
This is consistent with the opposite end of the spectrum when we look at the global businesses that say payroll data security has become "not at all important" over the last 12 months. As you might expect, the raw numbers are much lower, but they do reveal a statistically significant pattern.



Payroll data security incidents

Companies with a decentralised structure (managed by individual payroll teams) are twice as likely to have experienced five breaches or more than those in a centralised (shared service) structure (12% and 6% respectively).

How would you describe the cyber-attack security breaches that have impacted your payroll operation since the pandemic?



However your payroll team's structured, best practice is to formally assign information security responsibilities to one or more individuals who will be responsible for contacting authorities (e.g., law enforcement, fire department and regulators in the event that the security breach has violated a regulation) should an incident occur, and to have implemented a data security policy across your organisation.

What's the most secure set-up?

As you're thinking about the optimal organisational approach to managing payroll within your company's new market, consider whether setting up an in-country team or outsourcing to a single local vendor would work best for your organisation.

If your firm already has a shared services team in charge of multiple business units' payroll, a lot will depend on the amount of different payroll vendors and platforms that team is currently managing. Merely centralising, while continuing to add more local vendors, each with different technology, is unlikely to minimise the rising security risks to any global payroll program.

Of course, the robustness of the payroll technology itself is key (as we're about to see). However, as the survey results show, how you structure your payroll operations and service delivery also plays a big part in ongoing information security.

Payroll data security: the technical considerations

Identifying potential risks in your existing payroll system(s)

Before evaluating the data security landscape of your new overseas market, you will need a solid view of the whole payroll tech stack across your current countries.

Security requirements of information systems: have you identified and agreed on security requirements before you start to roll out payroll systems in your new geography? (These include operating systems, infrastructure, business applications, off-the-shelf products, services and user-developed applications.) [ISO 27002, 14.1]

Vulnerability monitoring and scanning: this includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for flow control mechanisms that are improperly configured or operating incorrectly. [NIST Special Publication 800-53]

In our Potential of payroll in 2024 research, 22% of business leaders say they've reviewed the effectiveness of their payroll systems over the last 12 months, while 20% say a review is currently underway.[1]

Before the expansion, you should consider the following critical areas:

- **HR/payroll digital maturity:** did your business quickly shift to digitisation or payroll digitalisation projects, perhaps because of pandemic-related pressures? Can you pinpoint the true maturity level of your existing payroll function?
- **International data transfer security:** have you mapped the various data flows of your employee payroll information, across national and international platforms and providers?
- **Audit trail functionality:** can you identify which employee(s) interacted with your company's payroll data and why?
- **Connectivity:** are your payroll platforms integrated with any other systems or applications, and have you assessed the security risk of this connectivity?

Using data from your organisation's existing countries will help you identify potential security gaps and quantify the risk before you extend your payroll function.

International and industry-based data security standards

There are currently a growing number of IT security and cybersecurity frameworks available that may serve as a useful blueprint for expanding businesses. The only auditable international standard that defines the requirements of an ISMS (information security management system), **ISO/IEC 27001** is one of the most well-known, while the United States' **NIST** (National Institute of Standards and Technology) **CSF** (Cybersecurity Framework) has also become a worldwide standard.

Depending on your business sector, you may be subject to specific industry standards, such as the **Sarbanes-Oxley (SOX)** act of 2002 covering US financial firms.

Payroll data security: the physical considerations

Non-malicious data threats and potential hazards in your new geography

Protecting your entire payroll data infrastructure means the physical components too — the IT infrastructure and physical environment housing your systems — which can be challenging if you're unable to supervise security measures on the ground in your new location.

When the expansion decision comes, ideally you want to be ready to deploy security measures already in place within your centralised operations, technologies and remote services in compliance with international security standard ISO 27001.

Examples of physical considerations

- Work premises and facilities
- Data servers (some countries have 'data localisation laws' requiring companies to keep a copy of certain data on local in-country servers)
- Equipment (e.g., workstations, devices), including disposing of physical media containing payroll data
  - 'Bring Your Own Device' (BYOD) — personal laptops, phones and tablets used for work purposes
- Supporting infrastructure, such as electrical supply and cabling

Environmental disasters

Events like fires, storms, earthquakes or even civil unrest can quickly disrupt or disable your payroll IT infrastructure.

Health-related threats

Public health crises such as the COVID-19 pandemic could impact payroll operations or compromise data security.

Controls to assess the risk

- Establish policies and train staff on preventing unauthorised physical access and interference in your company's premises and information, including your data hosting facilities.
- Set up special controls to protect on and off-site equipment to reduce the risk of unauthorised individuals gaining access to payroll data (and protect against loss or damage).
- If your new in-country staff are going to be working remotely and using their own devices (at least initially), make sure they have adequate endpoint protection for home and remote devices
- Review in detail the physical and environmental conditions of your new facilities, including fire hazards, HVAC, disaster susceptibility, access control, housekeeping, etc.
- Establish policies for sudden, mandatory mass evacuations and how valuable payroll security assets would be protected

The physical storage of payroll data

How will you store payroll records in your new geography? Most midsized and large businesses require automated or semi-automated digital recordkeeping, relying on payroll software to update records each time payroll is run and provide the reports and documentation needed for compliance. Whether you use the cloud or external hard drives, recordkeeping is ultimately your responsibility as an employer.

Ensuring the safety of this data in your new country will likely require local legal and compliance expertise. On top of data regulations like the GDPR, countries may have laws that mandate for how long firms should retain payroll records and how payroll data should be destroyed once the employee leaves the company (for example, laws relating to tax and pay equality).

Some countries even have so-called data localisation laws that require companies to keep a copy of certain data on local in-country servers. You'll need to consider whether legal experts are needed to advise your company and entrust the implementation of any requirements to a payroll partner with solid data security credentials.

Global payroll demands global protection — which is why ADP operates state-of-the-art Critical Incident Response Centres (CIRCs) located at strategic points around the world, all operating on one integrated platform. This 'follow-the-sun' model ensures constant vigilance and monitoring across continents and time-zones.

What can you do to improve your data security practices?

At both operational and strategic levels there are plenty of pre-emptive actions you can take to improve your security defences, using the security frameworks mentioned earlier as a starting point.

Read ADP global payroll security: protection you need from a partner you can trust to find out how we support our growing international clients all around the world.

> "What's a resilient and safe and secure way to run payroll? It turns out the best practice is to give it to someone who specialises in that."
>
> **Volker Schrank,**
> **Senior Director of Employee Experience and HR Technology, Mondelez**

Learn more at uk.adp.com

1. ADP, The potential of payroll in 2024: Global payroll survey.
2. UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT (UNCTAD), Cybercrime Legislation Worldwide, 2021.
3. U.S. Securities & Exchange Commission, Press Release, 2022.
4. EY Global Payroll Survey 2022.
5. ADP, The potential of payroll: Global payroll survey 2021.

DISCLAIMER: This document and the information contained herein are for informational purposes only. They should not be interpreted as advice, including legal or technical advice to take or to refrain from taking any particular action or to make or not make any decision, including but not limited to any administrative, technical or physical controls, or any hiring decisions.

Always Designing for People®