remote

IP and Data Protection Guide

A guide to protecting your intellectual property and sensitive data abroad.

READ MORE ↓

Protecting your IP and data with international employees

Employing a global workforce unlocks incredible potential for growth for your business — but global opportunities also bring significant global challenges.

Protecting your intellectual property and sensitive data is tricky enough in one country. Add multiple to the mix, and you now have to protect the interests of your company against a host of factors.

The stakes are raised. Even if you and your employees have the best intentions, you could accidentally land on the wrong side of international laws or expose your operations to attack from malicious sources.

At Remote, we know a thing or two about international employment. Our own team spans more than 50 countries on six continents, and we've helped countless companies employ people from all over the world. In this guide, we'll introduce you to some of the core concepts regarding IP and data security when you have workers in multiple countries.

Intellectual property protection

Why do you need to protect your IP?

There are several consequences for failing to protect your intellectual property:

01 You could lose sales and partnership opportunities

Companies want to work with partners they can trust. Lose control of your intellectual property, and others may view your business as more of a risk than an asset.

02 You could fail an audit

Liquidity events require companies to undergo extensive IP audits. If another company is looking to acquire yours, or if you are considering an initial public offering (IPO), you must be able to pass inspection from regulators. Nothing can derail progress like the discovery that your ownership of key pieces of IP is in question.

03 You could end up in the news for the wrong reasons

Your IP protections may be sufficient, but if there is any question of your ownership, a disgruntled employee or contractor may decide to challenge you in court. If that happens, your business may receive negative press, damaging your ability to recruit talent and work with new partners.

04 Your legal fees could skyrocket

Speaking of lawsuits, defending your company's IP in international courts can be enormously expensive. Not only do you have to pay massive fees for local legal representation, but your executives may have to spend days or weeks fighting cases — time that would be better spent growing the business.

05 You could even lose the IP for good

In some countries, ownership of work created defaults to the creator over the entity commissioning the work. A small detail in case law could jeopardize your entire operation if you are not careful. Better to protect your IP from the start than face the consequences later.

How does Remote protect your IP abroad?

Successfully protecting your IP rights insulates your business from harm while providing the security you need to grow your global team with confidence. Fortunately, Remote helps you maintain ownership of your IP no matter where you hire. We call this Remote IP Guard — the strongest global IP protections in the industry.

Learn more about: Intellectual property protections for Remote workers on the Remote blog

Remote IP Guard includes:

01

Fully owned entities and local legal experts in every country

Many employers of record (EORs) outsource their in-country hiring services to third parties. Remote does not. In every country where we operate, we own our own local legal entity, complete with local experts. This means that we know all there is to know about local IP laws and can protect your business from unexpected obstacles.

02

Ironclad two-step IP transfer process

Others pass your IP from one third party to another, exposing your business to risk at every turn. Remote cuts out every intermediary by following our two-step IP transfer process. The IP transfers from your employee to Remote and then to you, guaranteeing you the maximum transfer of IP rights no matter where your team members work. The IP remains legally yours from the very beginning, while our local legal experts handle the paperwork.

03

Maximum protections based on local legal precedents

You don't need to become an expert in international IP law to hire in other countries. With Remote, you can rest easy as our in-country teams of legal experts craft employee agreements that comply with all applicable local laws. No one else offers the same combination of local knowledge and legal expertise to keep your IP protected abroad.

Data security

Why is data security important?

Just like your IP, your sensitive data deserves to be protected from theft, corruption, and misuse. Failing to treat the security of your data with respect can lead to a host of problems:

You could be the victim of a ransomware attack

Bad data security means more opportunities for someone outside (or even inside) your organization to access and use that information for unintended purposes. That can range from minor issues to full-blown attacks, which can take your systems offline, permanently delete information, or carry substantial costs.

Your company could receive negative press

While bad IP protections can lead to negative press because of contentious court cases, bad data security can cause outside parties to question your organization's trustworthiness. The more secure your data, the more secure your reputation.

Your employees may lose trust in your business

Speaking of trust, a data leak can erode the trust of your most valuable audience: your team. Your employees need to believe that their sensitive personal information and their livelihoods are safe in your company's hands.

You may be subject to heavy fines and penalties

While governments typically do not punish companies for losing their own IP, they can and do punish companies for data breaches. When you have access to personally identifiable information of customers and employees, you are responsible for safeguarding that information. Failure to do so may result in a host of expensive problems.

You may have to delay or cease operations

In some cases, regulators may force your business to cease operations until you can prove you have rectified issues of data security. In others, a hacker could take important systems offline for days or weeks. You must protect your data to keep your operations running.

Which types of data need protection?

Different types of data require different types of security. Even if your company does not collect personally identifiable information from customers, you may still be responsible for protection of other types of data.

01 **Personally identifiable information (PII) of customers**

02 **PII of employees**

03 **Internal data**

- Strategic plans
- Documentation

04 **Confidential data**

- Legal documents
- Contracts and agreements
- Information about partners and vendors

05 **Restricted data**

- Code and codebases
- Banking information
- Other information required to be protected by law

Data security

How does remote help protect your data with international employees?

Remote offers the most robust data security in the industry. We understand the risks associated with bad data practices, so we integrate protection of sensitive information into everything we do.

In addition, Remote owns entities in every country where we operate, which means we never pass off your data through untrustworthy third parties. Read more about the differences between owned-entity and partner-dependent global employment solutions on the Remote blog.

01 Built-in platform security

- Remote's infrastructure lives in isolated networks with restricted, fully auditable access.
- Advanced firewalls and security threat detection and prevention insulate sensitive data from harm.
- Remote holds a number of security certifications, including SOC-2, to go above and beyond industry standards or legal requirements.

02 Internal security measures

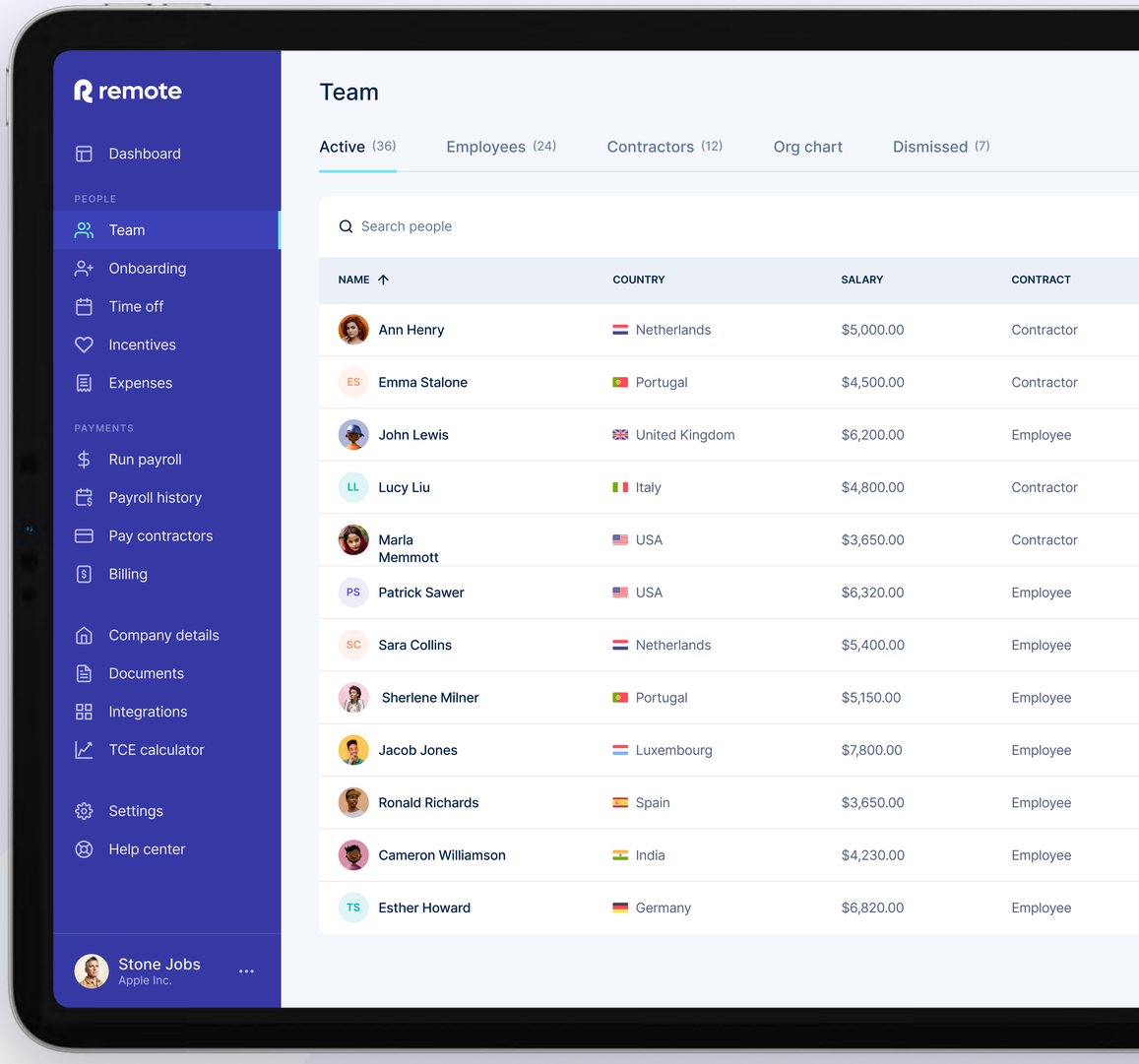
- Remote practices the principle of least privilege to ensure the fewest number of individuals necessary have access to sensitive data at any given time.
- All data handled at Remote travels only through auditable and secure channels, eliminating opportunities for accidental leaks.
- Remote employees only refer to data using platform profiles, so sensitive data is never revealed, even internally.

Expand your global team with peace of mind

Remote does not only understand the need to protect your sensitive data and intellectual property — we act on it. As the leaders in international employment, we offer the highest levels of IP and data protection for your growing global team. No one else can offer you the security, confidence, and care that Remote does.

While it's important to protect your business, you should not let the risks outlined here prevent you from expanding your team into new countries. Global talent can accelerate your business and help you achieve your goals in record time. With Remote, you can grow and hire internationally with confidence.

Learn more about how to employ internationally with confidence at Remote.com



Simplify your onboarding with Remote

Manage your global team with Remote to onboard and pay your new starters with ease.

GET STARTED NOW

remote