



Protecting Your Personal Data Globally

*How ADP's Adoption of Binding Corporate Rules
Helps Your Company Comply with the General
Data Protection Regulation*



A more human resource.®

“We’re passionate about protecting the privacy of our clients’ and employees’ personal information at every stage – as we define, develop and refine our products and set the policies that govern how we gather and manage data every single day. Implementing Binding Corporate Rules illustrates our commitment to protect personal data in accordance with the standards required in the EU, regardless of where the European data is processed, accessed or hosted.”

– Carlos Rodriguez, President and Chief Executive Officer, ADP

Why do companies like yours trust ADP with their most sensitive personal information? Because protecting your privacy and security is one of our founding principles. With the General Data Protection Regulation (GDPR) coming into force in May 2018 in the European Union, privacy regulations and laws continue to become more stringent. ADP is committed to keeping the personal information we process on your behalf secure, while staying on top of the GDPR and other legislative developments to meet the mounting compliance challenges of privacy and data protection.

We provide cloud-based human capital management and business outsourcing services to more than 700,000 companies, and employ over 58,000 people around the world. As a company, which must comply with privacy legislation covering the personal data we hold for our employees, and as a service provider to other companies whose data we hold, we prioritize individuals’ privacy and protection across our products and services. Countless companies simply wouldn’t trust us with their most confidential information otherwise.





The General Data Protection Regulation

Privacy Protection Reform for the Globalized Online Age

Officially taking effect from 25 May 2018, the GDPR aims to create a single data protection framework across the European Union; replacing local EU privacy laws and reducing the differences across EU Member States that existed under the previous regime. Simultaneously, the new regulation boosts the power of Data Protection Authorities and thrusts individuals' privacy rights to the top of the corporate agenda.

Introducing tougher requirements compared to most previous European laws, the GDPR has a major impact on organizations' data protection practices across the globe. Enshrined within its articles is the principle of accountability, which means your company must assess, demonstrate and document compliance with the GDPR on an ongoing basis. 'Data Protection by Design and by Default' is another core tenet. This tighter privacy environment is matched by much steeper penalties for data breaches (fines of up to €20 million or 4% of global annual turnover; whichever is higher).

How Will Your Company Transfer Personal Data Abroad?

If your company transfers personal data out of the European Union, you must choose a lawful mechanism for compliance under the GDPR.

The GDPR explicitly recognizes Binding Corporate Rules (BCRs) as an appropriate safeguard for transfers of personal data out of the EU. The region's Data Protection Authorities also recognize BCRs as the best path to compliance with the GDPR's accountability obligations.

WHO MUST COMPLY WITH THE GDPR?

- Companies located within the EU and companies located outside of the EU that offer goods or services to (or monitor the behavior of) EU residents
- All companies that process or hold the personal data of EU residents, regardless of the company's location





Binding Corporate Rules – An Internationally Recognized Standard for Protecting Personal Data

- BCRs are policies developed internally among a group of companies that share a common parent
- They provide a consistent set of rules on transferring the personal data of clients, employees and other individuals internationally, regardless of where such data is processed
- BCRs become legally binding once the EU Data Protection Authorities approve them (the DPAs are the regulators based in each of the EU's Member States)
- The GDPR expressly recognizes BCRs as a way to safeguard the transfer of personal data out of the EU
- Europe's Data Protection Authorities regard BCRs as the best option for protecting individuals' privacy rights in accordance with the GDPR requirements

ADP Achieves the Highest Standards of Global Data Protection

As of March 2018, ADP ranks among an elite group of companies worldwide to have gained regulators' approval to implement BCRs as both a data processor (covering the processing of clients' data) and data controller (covering the data of our employees and other business associates).

Why We Believe that ADP's Adoption of Binding Corporate Rules is Best for You

- **The 28 EU Data Protection Authorities have approved our BCR codes**, and ADP will continue to comply with our BCRs under the ongoing supervision of our Lead Supervisory Authority (the Dutch Data Protection Authority)
- As a BCR-approved data processor, ADP will assist you to **meet the highest standards expected by the European Union and you will avoid the cost and paperwork** associated with supporting data transfers through multiple model contract clauses
- Through ADP's BCRs, you gain a solution for transferring information about European data subjects that meets your multinational business needs, with the added **clarity and consistency that come from adopting a single global standard**
- **Our BCRs are embedded within ADP's existing global compliance policies and procedures**, providing your company's data subjects with an extra level of governance

The Pulse of Data Privacy Principles Across ADP

The touchstone of any effective data privacy program is its ability to evolve and adapt to ever-changing global data protection legislation. At ADP, we believe that a solid governance structure with clearly assigned accountability must sit at the heart of enterprise-wide data privacy initiatives.

To ensure compliance with privacy laws, including the GDPR and our Binding Corporate Rules, the Global Data Privacy Team spearheads privacy efforts across our organization. We have established a Privacy Leadership Council comprised of cross-disciplinary professionals including representatives of our business units.

These leaders play a vital role in promoting the importance of our privacy messaging across ADP, while designated business leaders, known as Privacy Stewards, take on management responsibilities for the controlled processing of your personal data within each ADP business unit and function.

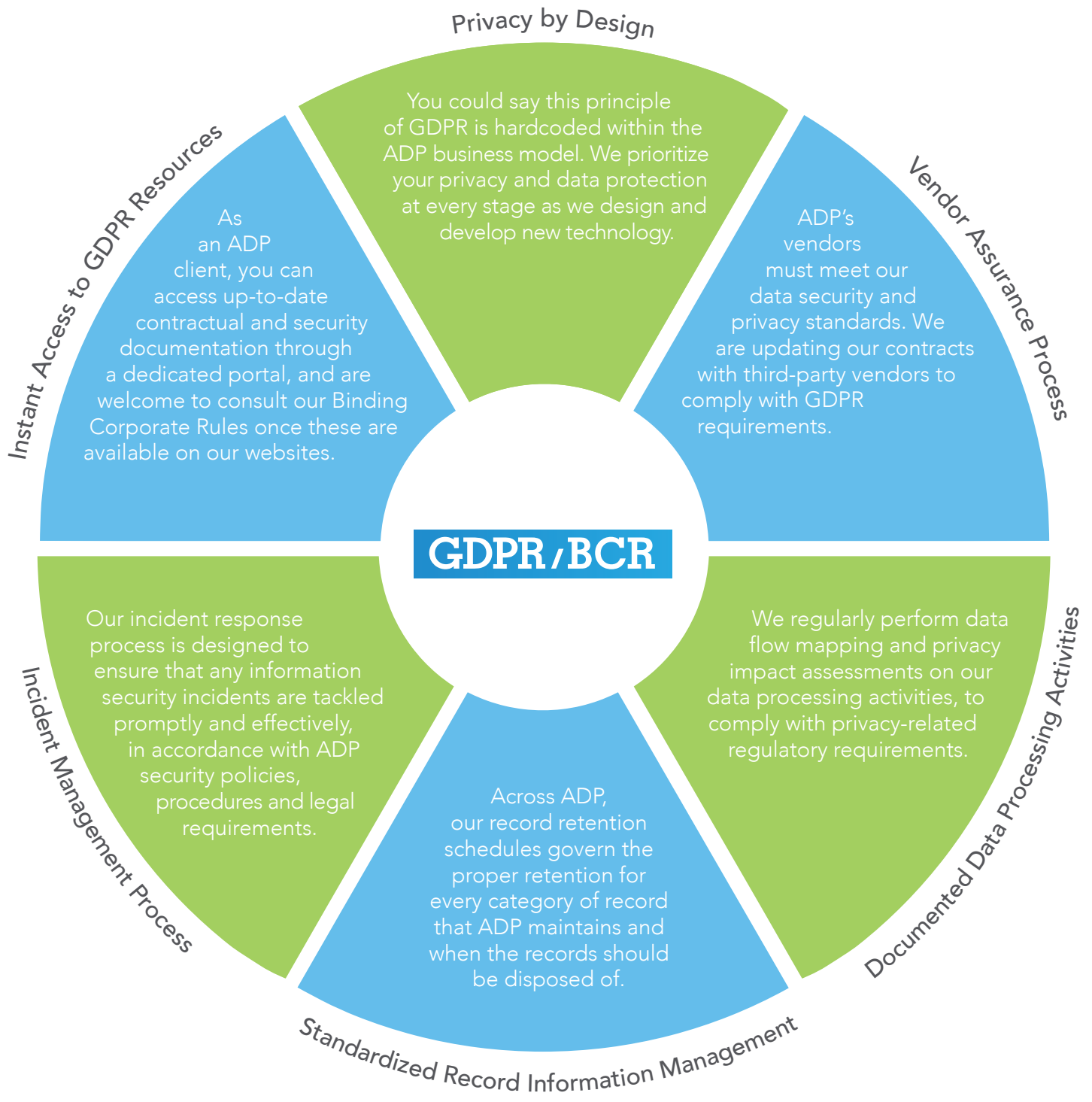
We've found that this approach succeeds in generating a collective energy around data privacy compliance – becoming something much more than a pure privacy or compliance project, and involving all ADP departments in our data protection action plans.

ADP's Privacy Policy Applies to all Affiliates and Employees Worldwide



Your Privacy is our Priority

ADP's decision to adopt Binding Corporate Rules reflects our commitment to the highest standard of safeguards for your employees' personal information. Our Privacy Program revolves around the GDPR's principles and our BCRs.



FAQs around Binding Corporate Rules (BCRs)

Our company has Standard Contractual Clauses (SCCs) – are these effectively the same as BCRs?

Both SCCs and BCRs are valid approaches to comply with GDPR data transfer regulations, but there are several differences between the two. The most important distinction is that all the parties that receive the personal data need to sign separate SCCs for each and every transfer to third countries (even within an international group). BCRs are policies internal to a group, validated by the EU's Data Protection Authorities and made available to clients and individuals. Once they're in place, they mean you're compliant to carry out all data transfers that their scope covers.

Why has ADP chosen BCRs as the preferred route to GDPR data transfer compliance?

Previously, our data transfers were based on EU Commission's model contracts, which was a cumbersome solution that added complexity to the contracting process with our clients. A natural extension of existing corporate compliance policies and procedures, BCRs simplify the data transfer process, as our clients are no longer required to sign model contracts for every data transfer.

BCRs are the most robust mechanism for intragroup data transfers because beyond the policy itself, they're reinforced by a compliance program including associates' training and audit. They also give you the added reassurance of knowing that regulators (the EU Data Protection Authorities) have reviewed a company's privacy compliance program.

If my service provider, such as ADP, already has EU accreditation for their BCRs, does my company need to secure this approval as a data controller too?

As long as your company uses providers who can meet the GDPR's data processor obligations concerning data transfer to third countries, you as the data controller don't need to adopt BCRs as well.

Contact ADP's Global Data Privacy and Governance team

If you'd like to find out more about ADP's approach to GDPR and Binding Corporate Rules, you can reach our team at privacy@adp.com. To learn more about how ADP protects data, visit adp.com/trust.





A more human resource.®

Many thousands of multinational enterprises and employees worldwide trust ADP with their most sensitive personal information every single day. As a BCR-approved data processor, ADP has been recognized by European regulators as a trusted and accountable custodian of your data within this new era of European data protection governance.

ADP, the ADP logo, and ADP A more human resource. are registered trademarks of ADP, LLC.
All other marks are the property of their respective owners.
Copyright © 2018 ADP, LLC. All rights reserved.