



ARMOR BULLETIN - GLOBAL REGULATIONS: FALL 2020

UPDATES ON GDPR



The General Data Protection Regulation, or GDPR, represents one of the most influential pieces of data privacy and security legislation ever enacted. Though GDPR's scope is to protect privacy for citizens of the EU (wherever they may be), its impact is felt across companies worldwide that are doing business in the EU, or may be engaging and collecting data on EU residents.

As a cybersecurity software company specializing in securing sensitive applications and data for organizations subject to compliance with GDPR, Armor is often asked about the latest developments associated with GDPR. As a result, we are providing this bulletin to bring organizations up to speed.

FROM THE TOP



We can't expect of each individual who just wants to read an interesting article to go through terms and conditions and catch if something's wrong. We need authorities, we need strong enforcement, because only then will the right to control your data become a reality in people's lives, and only then can we start to restore Europeans' trust in a digital world.

— Margrethe Vestager

Executive Vice President, European Commission for A Europe Fit for the Digital Age

CONTENT

THE ENFORCERS	3
A SILVER LINING	3
GUIDANCE FOR 2021	5



THE ENFORCERS

Forrester reports that as of January 2020, Data Protection Authorities (DPA) levied 190 fines and penalties related to non-compliance with GDPR since its implementation in 2018.

Forrester's research noted:

■ Enforcement Drivers

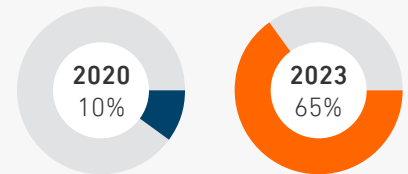
Data governance failures, security lapses, and failure to notify proper channels of a breach were the leading causes of fines and penalties. Enforcement actions to date are just the beginning with much more to come.

■ A Single Record Matters

The penalty for mishandling customer and patient data for a single customer or patient record resulted in fines as much as \$45,000 to \$120,000.

The takeaway is clear: Organizations must take GDPR compliance very seriously or risk hefty penalties for even the smallest of infractions and non-compliance.

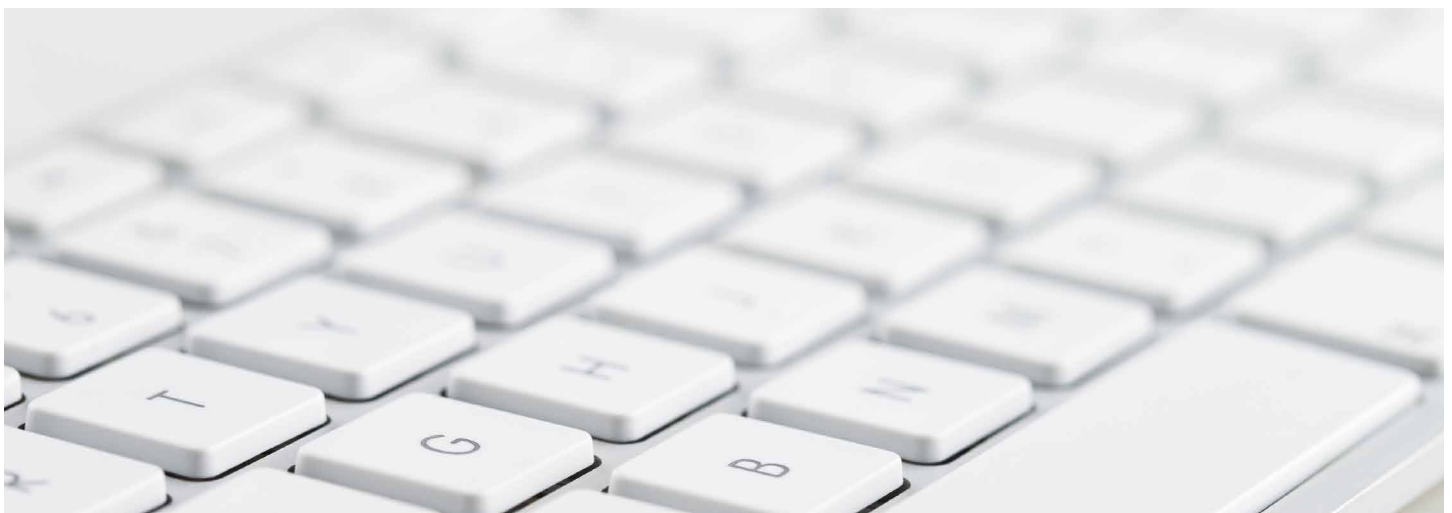
THE DATA PRIVACY REVOLUTION IS JUST BEGINNING



Gartner, Inc. estimates that personal data for as much as 65% (versus 10% today) of the world's population will be subject to some form of data privacy legislation by 2023.

A SILVER LINING

GDPR compliance is not all work and no rewards. When executives were surveyed on their compliance with GDPR and a number of other areas, Capgemini Research Institute revealed a link between proactive GDPR compliance efforts and enhanced business performance. In fact, we found it fascinating that 92% of executives surveyed in a Capgemini Research Institute report indicated their organizations had attained a sizable competitive advantage (see below) as a result of their proactive compliance with GDPR.





PERFORMANCE & GDPR



BREXIT & GDPR

Though the United Kingdom officially left the EU on Jan. 31, 2020, GDPR is still very much in effect for citizens of the UK. At some point, the UK and EU will need to negotiate a new framework between the two bodies. It is unclear if the UK will have an agreement or new framework in place on Jan. 1, 2021. However, the Information Commissioner’s Office (ICO) has published guidance for businesses on its website, and we recommend companies, in particular UK-based organizations, review the site and continue to keep tabs on updates as we approach the new year.



For now, and even if GDPR is no longer in effect for the UK in the future, Armor recommends businesses continue to follow GDPR principles and practices for UK citizens in anticipation of some level of new agreement, as well as to minimize any risk associated with collection and security of personal data on UK citizens and EU citizens living in the UK.

Check out the [Information Commissioner’s Office website](https://ico.org.uk) for more information.



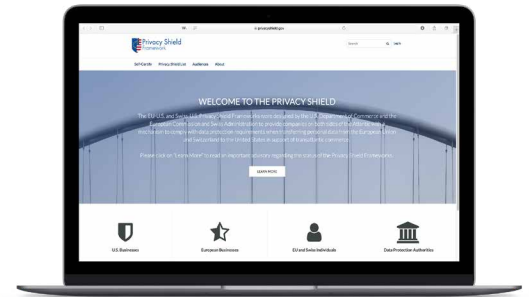
PRIVACY SHIELD FRAMEWORK

If you are familiar with what is happening around the Privacy Shield Framework, or even if you are not, we thought the language below—direct from the Privacy Shield website—sums up the latest with regard to the framework and its relationship to GDPR:

*“On July 16, 2020, the Court of Justice of the European Union issued a [judgment](#) declaring as ‘invalid’ the European Commission’s Decision (EU) 2016/1250 of 12 July 2016 on the adequacy of the protection provided by the EU-U.S. Privacy Shield. As a result of that decision, the EU-U.S. Privacy Shield Framework is **no longer a valid mechanism to comply with EU data protection requirements** when transferring personal data from the European Union to the United States. This decision does not relieve participants in the EU-U.S. Privacy Shield of their obligations under the EU-U.S. Privacy Shield Framework.*

The U.S. Department of Commerce will continue to administer the Privacy Shield program, including processing submissions for self-certification and re-certification to the Privacy Shield Frameworks and maintaining the Privacy Shield List. If you have questions, please contact the European Commission, the appropriate European national data protection authority or legal counsel.”

We recommend keeping tabs on [Privacy Shield Framework’s website](#) for any updates.



GUIDANCE FOR 2021

▪ **Tighten the Ship or Loosen the Wallet**

For organizations subject to compliance with GDPR, given indications of strong enforcement actions to continue into the future, we recommend performing a review of policies and processes to heighten confidence that your organization’s security and privacy practices are compliant with GDPR requirements.

▪ **Keep One Eye to the UK and the Other to the EU**

As we mentioned earlier, with the end of the transition period, the UK and EU will need to adopt a new privacy and security framework to put in place on Jan. 1, 2021. Because we don’t yet know the full outcome of this effort, or whether new legislation will be in place by the deadline, we recommend organizations keep close watch for updates and developments cited on the Information Commissioner Office’s website as well as on EU GDPR channels.

▪ **Data Subject Access Requests**

Organizations should prepare for how to effectively satisfy Data Subject Access Requests, or DSARs, at some point in the future if they have not already. Individuals now have a mechanism whereby they can exert greater control over the information organizations have collected from them. Individuals in the EU have “the rights of access, rectification, erasure, and portability of their personal data, the right to object to a processing, as well as enhanced transparency.”

This is an area of compliance with GDPR that could create a flood of requests, complaints, and potential suits filed against companies related to their data collection and use practices. We recommend processes be put in place to recognize, expedite, and automate proper handling of DSARs to minimize risk to organizations.



▪ **Cross-Border Data Transfers and Standard Contractual Clauses**

GDPR did not do a good job when it came to addressing cross-border data transfers. Standard Contractual Clauses (SCC) were not effective in capturing actual use cases and scenarios related to data transfers. This is an area the Commission to the European Parliament and the Council has vowed to improve upon, and we should see some movement and results in 2021.

▪ **Be Mindful of Third-Party Relationships and Risk**

We recommend that organizations sharing data with third-party firms possibly regulated by GDPR should take a hard look at their vendor relationships. Using a partner or affiliate for handling and/or processing sensitive data could introduce risk if there is an indication the third party is not appropriately in compliance with GDPR. Because of the serious enforcement of GDPR the EU is taking, organizations may want to consider prioritizing vendor audits where GDPR compliance plays a role.

ABOUT ARMOR

Armor is a global cybersecurity software company. We simplify protecting data and applications in private, public, or hybrid clouds as well as help organizations comply with major regulatory frameworks and controls. We know security is complex; it doesn't have to feel that way.

To accelerate your compliance with GDPR, check out [Armor](#).

SOURCES:

- "Guess What? GDPR Enforcement Is On Fire!," Forrester – January 28, 2020
- "Vestager from DPC: Enforcement critical to success of GDPR," International Association of Privacy Professionals (IAPP) reporting on events at IAPP Congress meeting – November 21, 2020
- "Gartner Report: 65% of the World Protected by Data Privacy Legislation by 2023," Compliance Junction, citing Gartner research presented in September 2020 – September 15, 2020
- "Championing Data Protection and Privacy: A source of competitive advantage in the digital century," Capgemini Research Institute – Based on June 2019 survey data
- "How the GDPR could change in 2020," GDPR.EU – 2020
- Privacy Shield Framework – <https://www.privacyshield.gov/welcome>
- Information Commissioner's Office – <https://ico.org.uk/>
- "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation," European Commission – June 24, 2020.



[ARMOR.COM](https://armor.com) | (US) +1 844 682 2858 | (UK) +44 800 500 3167

20041118 Copyright © 2020. Armor, Inc., All rights reserved.