

## CEP Magazine – January 2021

# Your organization has received a data access request. What now?

---

By Patrick O’Kane

**Patrick O’Kane** ([patrick.okane@fisglobal.com](mailto:patrick.okane@fisglobal.com)) is a London-based UK Lawyer (Barrister) and Data Protection Officer for a US Fortune 100 company.

There has been something of a tsunami of privacy regulation over the past few years, and this is set to accelerate. According to Gartner, 10% of the world’s population in 2020 had a modern privacy law regulating the use of personal data, and it predicts that by 2023, 65% of the world’s population will have a modern privacy law.<sup>[1]</sup>

Since 2018, we have had major privacy laws implemented: the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the US, and the General Data Protection Act in Brazil. A major new privacy law is expected in India—the Personal Data Protection Bill—in 2021.

These regulations have many features in common, including security requirements, large penalties and fines for breaches of the regulation, and privacy notice requirements. They also share an important common feature. They give individuals the right of access over their personal data. Under privacy regulations, an access request is usually a right for an individual to access and receive a copy of all of the personal data your company holds on them. This may include any record containing their name or information.

### Knowledge is power

In the movie *My Cousin Vinny*, the inexperienced but streetwise defense lawyer Vinny Gambini is trying his first murder case against an experienced prosecutor. “I’d sure like to get a look at your files,” he says to the prosecutor. Vinny is delighted with himself and feels he has been very skillful when the prosecutor immediately grants him access. Vinny, in his naivete, doesn’t know that he had a legal right to access the files all along.

More and more individuals are learning about their own legal right to access their personal data, so it is becoming more prevalent on a global scale.

### The challenges of the right of access

In the digital age, data are the new oil, and companies are keen to drill for as much as possible. Privacy regulations want to control the flow of that oil and ensure that privacy rights and freedoms are upheld.

Companies face many challenges in dealing with access requests because there are two competing interests at work. Regulation, in the form of GDPR, wants to limit personal data processing and to give individuals access to their personal data. Conversely, companies want to slice, dice, and commoditize as much personal data as they can with limited interference.

Companies hold all sorts of information about people, from marketing and human resources data to the most sensitive information relating to a client’s conduct, finances, or health. Personal data can be held in myriad different forms across multiple locations.

Much of the personal data may be held off premises, including data held in the public cloud. Personal data are

---

often held by a multiplicity of vendors and business partners. They come in various shapes and sizes, such as customer call recordings, security camera footage of individuals, purchase history, records of website activity, paper records, etc. Then there is the dreaded email. One United Kingdom access request made by an employee to their employer necessitated the review of 500,000 emails at a cost of \$150,000.<sup>[2]</sup> The burden of dealing with these requests can cost companies up to \$2 million a year.

There is also the problem of identity checks. The BBC News site reported a case where a University of Oxford researcher decided to conduct an experiment on access requests.<sup>[3]</sup> He contacted 83 companies pretending to be his fiancée. His fiancée had agreed to participate in the experiment and allowed him to see if he could obtain her data from various companies. Of the 83 companies he contacted, 24% supplied him the personal information of his fiancée.

## How does my company deal with access requests?

The rules on access requests under GDPR and CCPA have high expectations. They expect that you can find all the data on a particular person within a strict time limit (one month under GDPR and 45 days under CCPA).

There are three steps you can take to ensure access requests are dealt with properly within your company.

1. **Stay on top of records management:** Records management is too often ignored within companies. Companies must ensure that records and data are subject to deletion time limits. Otherwise obsolete data can accumulate and cause risks and liability to companies, particularly if the data are the subject of a security breach. Put strict time limits in place around the retention of data within your company and enforce those time limits vigorously.
2. **Put a written procedure in place:** This is an instruction manual on how your company will deal with access requests. The procedure for dealing with access requests should include:
  - Details on how individuals can make an access request.
  - How the person's identity is verified before granting the request.
  - How the company should search for the data.
  - How the data are reviewed before they are sent out.
  - How the data are sent out securely.
  - How staff are trained on access requests.
3. **Train, train, train:** Many of your staff will interact with individuals and customers. Would each of those staff members know what to do if a customer said to them, "I want a copy of my data," or, "I want to access all my data"? They should know because that customer has just made an access request, and the clock is now ticking. All staff should have some general knowledge of access requests, and this could be included in your general privacy training module. Some departments will require more detailed knowledge of access requests as they relate to their department. For example, human resources will need to be trained on handling employee access requests. Information technology may need to be trained on finding and accessing data across many different systems.

## Stay ahead of the privacy law tsunami

Dealing with access requests is a big part of privacy compliance. And with the deluge of privacy regulations

---

expected over the next three years, companies must act now to ensure they have the appropriate systems and controls in place to deal with these requests.

## About the author

**Patrick O’Kane** has helped lead a major GDPR implementation project across a group of more than 100 businesses and previously led the privacy team at a large group of insurance companies in London. He is the author of *A Practical Guide to Managing GDPR Subject Access Requests* and *GDPR – Fix it Fast: Apply GDPR to Your Company in Ten Simple Steps*, is certified in European Union and US privacy regulations, and was made a Fellow of Information Privacy by the International Association of Privacy Professionals in 2020.

## Takeaways

- Ten percent of the world’s population is currently covered by a modern privacy law, and the number is predicted to increase to 65% by 2023.
- Companies are collecting more data. There are rights under new and upcoming privacy regulations for individuals to access and obtain a copy of their data.
- In order to manage access requests, companies must ensure they are deleting old data from their systems regularly.
- It is important to put proper procedures in place to ensure your company can find, redact, and transfer data to the individual.
- Your staff must be trained to be able to recognize, escalate, and deal with access requests from customers and staff.

**1** Laurence Goasduff, “Gartner Says By 2023, 65% of the World’s Population Will Have Its Personal Data Covered Under Modern Privacy Regulations,” news release, Gartner, September 14, 2020, <https://gtnr.it/3escH2x>.

**2** *Deer v University of Oxford* [2017] EWCA Civ 121.

**3** Leo Kelion, “Black Hat: GDPR privacy law exploited to reveal personal data,” BBC News, August 8, 2019, <https://bbc.in/3l2R7E6>.

This publication is only available to members. To view all documents, please log in or become a member.

[Become a Member Login](#)