A review of the past month’s news stories related to Personally Identifiable Information (Pii) and other Privacy matters.
The short answer to this question is Yes, it does. The legislation provides guidance on what can and cannot be done with employee information or personal data (i.e. any data in the company’s possession that can identify the individual).

The legislation gives the individual control over his/her personal data i.e. control over how the data is used and what happens to it after it is used. It also gives greater accountability by stipulating what companies can and cannot do with the personal data that they have.
A family safety app used to track children’s movements is selling location data to several different data brokers, according to an investigation by The Markup.
Recently, in Canada, thieves have been using AirTags to track luxury cars to their driveway before stealing them. Apple had said that it would try and “fix this” back in June this year, and a solution of sorts has arrived, for Android users. The app called ‘Tracker Detect’ is available on the Google Play Store and can be used to set up and manage AirTags.

Source: https://www.businesstoday.in/technology/news/story/apple-rolls-out-a-tracker-detect-app-on-android-for-airtags-315555-2021-12-14
There are a number of settings on your iPhone and, if you’re like many people, you’re ignoring half of them. That’s perfectly fine (in most cases). But one place where it isn’t doing you any good is when it comes to your privacy. Some phone settings are literally giving away personal information about your whereabouts and daily habits and routines that you would probably rather keep to yourself.

Source: https://www.shefinds.com/collections/setting-turn-off/amp/
A summary of an action brought by WhatsApp Ireland Ltd. to the Court of Justice of the European Union (‘CJEU’) siting the European Data Protection Board:

• infringed Article 4(1) of the GDPR by interpreting and applying this provision and the term 'personal data' excessively;
• ... and others
If you've been on Facebook over the last few days, you've probably seen the '10 Year Challenge' pop up. While it may seem harmless, taking part could make you vulnerable to hackers. It's called data mining, and many cyber security experts say it's a sneaky way for hackers to take over your computer.

Google is calling on lawmakers in the US and Europe to establish new rules for a secure data transfer framework.

The issues between US tech companies and the GDPR have been ongoing. Last week, the Austrian Data Protection Authority (DSB) decided that a local Austrian website breached the GDPR by using Google Analytics. The DSB said that Google Analytics did not provide an adequate level of protection for users' data.
The FBI says cybercriminals are trying to steal your financial information through QR codes. QR codes have become increasingly more popular during the pandemic thanks to their ability to offer touch-free menus at restaurants and bars– but it’s the latest way cybercriminals are targeting your information.

QR codes are bar codes you can scan right on your phone to launch a website.

Scammers are using fraudulent QR codes to direct people to malicious sites in order to steal your personal information.

Facebook parent company Meta stands to lose $10 billion this year due to a small, but impactful change Apple made last year.

In April 2021, Apple enabled iPhone users to choose which apps are allowed to track their behavior across other apps. As a result, the vast majority of users opted out — which Meta CFO David Wehner said is hurting Facebook's ad revenue.

Morley Companies, an organization that provides business services to dozens of Fortune 500 companies, said this week it was hit with a ransomware attack last year that led to the leak of sensitive information for more than 500,000 people.

In a press release, the company said the ransomware attack began on August 1 and made their data "unavailable." Despite requests for comment, the company would not explain why it waited until now to notify the 521,046 people affected, some of whom had their Social Security numbers leaked in the attack.

Meta is considering shutting down Facebook and Instagram in Europe if the company isn’t allowed to process data from European users in the U.S. The company made this pretty serious threat in its annual report for the Securities and Exchange Commission, where it addressed the “complex and evolving U.S. and foreign laws” that could “harm” Meta’s business.

In the report, the company emphasized the need to find a new transatlantic data framework to transfer data from European users to the U.S. after the Privacy Shield was invalidated by the Court of Justine of the European Union in July 2020.

The End