Meeting GDPR needs with the PxM Platform

General
Data
Protection
Regulation

Whilst every cybersecurity company out there claims that they address GDPR requirements, Osirium's PxM Platform actually does. This informative piece explores how we help companies meet the 6 principles of GDPR, taking each in turn…

Principle 1. Lawfulness, fairness and transparency

"a) processed lawfully, fairly and in a transparent manner in relation to individuals;"

The first principle of GDPR – lawfulness, fairness and transparency – is truly the essence of GDPR. How the PxM Platform practically helps with the other 5 GDPR principles provides the evidence for how we help demonstrate lawfulness, fairness and transparency.

Principle 2. Purpose limitations

"b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;"

Deciding on the purposes of data collection is for the organisation to decide. Companies must set a framework in which the data will be accessed, processed and eventually deleted. This is the organisations GDPR policy. The PxM Platform can be understood as a 'policy enforcement'

cont. overleaf

Osirium is a UK software development team that has pioneered the concept of a virtual air gap for privileged account access. The team have delivered a virtual appliance that can recognise an incoming identity, create a connection to a system, device or application, perform single sign-on and enterprise class password lifecycle management, and then hand the pre-prepared session back to the incoming request ready for system management. The session can be recorded, subject to time windows and device group separation. We have delivered millions of privileged tasks and sessions for many of our blue chip clients. Osirium currently has four patents pending.

product. Whilst many other products focus on protection, the PxM Platform goes beyond this, implementing policy whilst keeping human elements away from the most vulnerable methods of data access.

Principle 3. Data minimisation

"c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;"

Principle 3 is a qualifier to the policy in principle 2. The 'limited' part of this principle is perfectly enforced by the PxM Platform's Privileged Task Automation functionality. It is not always necessary for an individual to have full access to a database. For example, their work may require that they deal with the customer who is currently on the phone. Using the Privileged Task Management module of the PxM Platform, a task can be created whereby data is retrieved that is adequate, relevant and limited to the task at hand. This approach prevents either the individual, or anyone else who has stolen that individuals credentials, from stealing the whole database.

Principle 4. Accuracy

"d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;"

This is the part of the policy that relates to timeliness and accuracy. The PxM Platform can help where customer service provisioning is complex with many parameters. We've used task automation to mask parameters that shouldn't be touched and to input sanitise key parameters.

Principle 5. Storage limitations

"e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;"

This relates to the underlying systems rather than what Osirium can do.

Principle 6. Integrity and confidentiality

"f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

This is the big one, the one that all cybersecurity companies argue that they help with. At its core Osirium does two things:

Identity In – Role Out

This approach speaks right to the essence of the sixth principle. Your organisation will be able to identify who has access to what even when 'shared accounts' are used. Identity gives a much better level of protection than giving humans access to privileged account credentials. It's sobering to consider that 99.9% of all data breaches involve privileged accounts.

Delegate the Task, not the Privilege

This is achieved through our Privileged Task Management module and is the strongest form of data security. Users no longer have direct access to systems, devices or applications. They cannot make bulk data copies or change underlying access rights.

One last thing...

Article 5(2) requires that:
"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

The PxM Platform provides an overview of who can use what tools, on what systems, where, and when. This means that visualisation of the GDPR policy enforcement is straightforward. Article 5(2) is also a reminder that if you outsource data functions, your organisation is still responsible.