Willis Towers Watson

The EU's General Data Protection Regulation (GDPR)

Is the Energy and Natural Resources industry ready?

What is GDPR?

On April 14, 2016 the European Parliament voted to adopt a new data protection law for Europe, the General Data Protection Regulation (GDPR). The regulation will come into effect on May 25, 2018.

The purpose of the regulation is to further harmonise national data protection laws across the EU, strengthen the obligations on those who use personal data, and enhance the rights of individuals.

The GDPR…

- Applies to all companies, inside or outside the EU, that target or monitor EU individuals or provide services into the EU
- Enforces fines of up to €20 million or 4% of global turnover, whichever is greater
- Imposes a 72 hour window for companies to report a breach if there is risk to affected individuals
- States that where an individual's consent is deemed necessary for the processing of data, that consent must be unambiguous and informed
- Affords individuals the 'right to be forgotten' in certain cases, and enhanced rights of access to their personal data
- Implements 'privacy by design' – privacy can no longer be an afterthought to operations
- Applies a more prescriptive statutory regime to data processors
- Sets up a 'one stop shop' – companies only have to register with one data protection agency
- Requires some companies who systematically process data to appoint a Data Protection Officer (DPO)

Why is it relevant to Energy and Natural Resources (ENR) companies?

By virtue of their global operations, large workforces and complex supply chains, ENR companies hold access to large quantities of EU citizens' personal data

- **Employees**: In addition to their workforce employed in the EU, ENR companies routinely deploy expatriate staff to fill capability gaps in non-EU operations. Many of these expatriates are citizens of EU countries
- **Suppliers**: ENR companies globally make extensive use of consultant suppliers – individuals employed to carry out defined tasks in niche specialist areas, perform time-bound roles on large capital projects, or fill temporary staff positions. A large proportion of these consultant suppliers tend to be EU citizens
- **Customers**: Within their European operations, many ENR firms will hold vast amounts of customer data. For instance, fuel retailers will have access to customer refuelling patterns and shopping behaviour through loyalty card programmes, while power suppliers will know customers' energy usage and bank account details

What are the key risks for ENR companies?

ENR companies face a unique set of risks in protecting the confidentiality and controlling the use of the data they hold on EU citizens

- As providers of critical and sometimes security-sensitive national infrastructure, ENR companies' operating facilities are prime targets for cyber-attacks. Depending on the motives and sophistication of the attackers, a breach could lead to significant data leakage, culminating in fines under the GDPR and a reputational impact
- ENR companies increasingly operate in less developed parts of the world with scarce local skills, making the presence of EU expatriates inevitable. These remote operations are organised as joint ventures, adding a layer of complexity to their workings. Setting data privacy policies globally to apply across all regions, and policing their implementation and effective use, is highly challenging
- Where local attitudes to data privacy and protection in far-flung geographies are of a lower standard of rigour to EU norms, local employees could, by carelessness or design, cause data breaches

What could ENR companies do to strengthen their data protection and reduce the risk of GDPR non-compliance?

With fines of up to 2% - 4% of turnover and reputational damage at stake, ENR companies could consider a series of steps to protect themselves from data breaches and the risk of falling short of GDPR requirements

- **'Privacy by design' principles could be rigorously tested** across the breadth of operations and new ventures. Operating assets could be tested as if a breach has taken place, being able to demonstrate in such circumstances that proactive risk mitigation measures were in place to safeguard against personal data loss. New ventures could consider building privacy-by-design into their asset development plans
- **Compelling global communications could be created and cascaded** to convey the consequences of data breaches, and accountabilities for breaches agreed at local levels. Companies could conduct culture surveys and risk assessments to identify local operations which might be most prone to divulging personal data - either deliberately or erroneously - and focus on these assets first
- Mandatory reporting requirements will increase publicity of failings, which could lead to reputational damage in addition to punitive fines. ENR companies could consider **preparing robust external communications strategies** to rapidly respond to a potential fallout, and explore innovative risk management and transfer solutions (such as greater use of Captives) that minimise the financial impact
- The GDPR also states that companies must **appoint a Data Protection Officer (DPO) i**f certain conditions are met. The DPO must have "expert knowledge of data protection law and practices", and report at Board level. This is a non-traditional skillset in limited supply, and we anticipate fierce competition in the wake of GDPR implementation, with the International Association of Privacy Professionals (IAPP) estimating a need for 28,000 DPOs in Europe alone. ENR companies must consider moving quickly to appoint a qualified DPO, giving them far-reaching authority to conduct global audits, recommend and rapidly implement policy changes

Contact
Thorsten Querfurt
Global Head of Natural Resources
+44 (0) 203 124 6236
Thorsten.Querfurt@WillisTowersWatson.com