

Deloitte.

DIGITAL REGULATION SURVEY

It's time for a new approach



FROM UNCERTAINTY TO CLARITY

From a societal perspective, our digital landscape has never been so important. Inextricably linked to everything that we do, and ever-evolving, it is no surprise that regulation is fighting to keep up with the pace that technology is setting. Often viewed as stifling innovation, this current wave of regulation is set to be a game changer if approached as it is intended: to enhance, support and drive innovation while safeguarding society as a whole. With 2025 set to be the year of digital regulation implementation, the Deloitte **DIGITAL REGULATION SURVEY** provides key insights from Irish based digital regulation leaders leading the charge across all lines of defence. Against the backdrop of geopolitical uncertainty, continuous moves towards efficiencies in the technology sector, as well as a multitude of converging and overlapping high impact regulation, leaders are looking for clarity, consistency and guidance.

Key challenges include uncertainty around the overall digital regulation focus being driven by the current political landscape and how the global tech platforms will react to this, a perceived lack of coherence across the multiple regulations across the EU, the availability of skills and talent in Ireland, internal management support, and the impact of the regulations on innovation and competitiveness in Ireland and the EU. However, with these challenges also comes opportunity to take stock and strategically look at the digital landscape and emerging technologies, how these will continue to evolve with a focus on driving innovation and how an equally innovative approach to compliance can be established to support current but also future regulation.

Here we set out the key themes from our survey results:

DIGITAL TRUST

Regulatory Impacts & Challenges

DIGITAL TRUST

Regulatory Impacts & Challenges

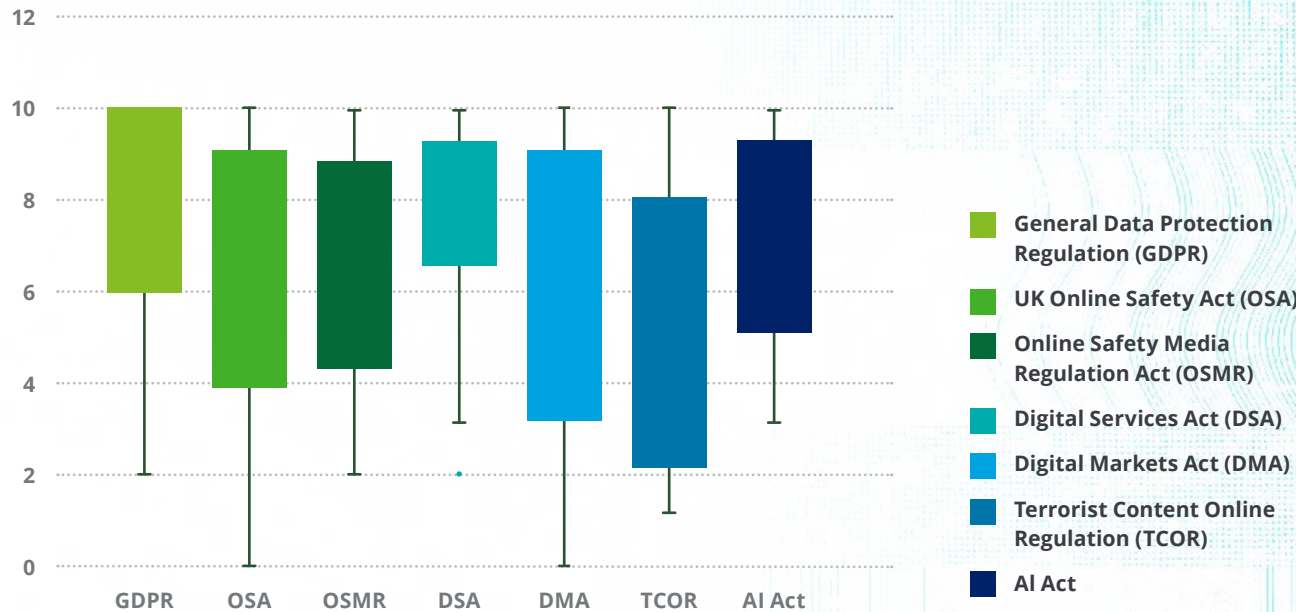
High Impact Regulations

High Impact Regulations:
The General Data Protection Regulation (GDPR) continues to have a high impact on business while newer regulations such as the Digital Services Act (DSA) are highlighted as having substantial impacts on businesses. The AI Act is emerging as a major concern due to its extensive requirements and obligations.

Fragmentation and Coherence

A significant concern for the industry is the fragmentation and incoherence of regulations between local Irish and EU levels. Tech firms express frustration over perceived lack of coordination, which complicates compliance and operational processes.

Q4. Rank the impact of each regulation relative to each other on your business
From 1 (low impact) - 10 (high impact)



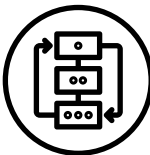
OUR HOLISTIC APPROACH

Our survey participants indicated that the General Data Protection Regulation (GDPR) is still ranking as the highest impact for their organisations. In fact, the GDPR is viewed as having set the precedent for the newer regulations with clear overlaps in areas such as transparency and the protection of data. In July 2024, the European Data Protection Board (EDPB) released a statement highlighting that the AI Act and all data protection legislation must be “considered (and coherently interpreted) as complementary and mutually reinforcing instruments”. To this extent there is a rising concern that AI Act compliance will quickly draw attention to legacy non-compliance with the GDPR. Building on the view that there needs to be coherence between digital regulations, the EDPB’s statement in December 2024 reinforced that the EDPB would “support a holistic methodological approach for the next evaluation of the GDPR that explores the interplay between the GDPR and other EU digital legislation”.

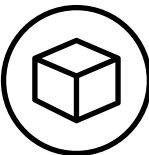
It is evident that a fragmented and siloed approach to Digital Regulations as a whole, will only create more challenges than solutions, leading to inefficiencies, higher compliance costs, open (and potentially higher) risks and ineffective remediation programmes. A holistic approach is required which should include:



An organisation-wide Digital Trust Strategy, ensuring that Global differences and overlaps are considered;



A future-proofed compliance framework with continuous horizon scanning and cohesion and collaboration across lines of defence, from the boardroom to operations;



A proactive ‘by design’ model, building trust into digital products and services as fast as the technology is being developed; and



A strong data governance model underpinning it all.

SPECIFIC REGULATORY CONCERNS

SPECIFIC REGULATORY CONCERNS

Age Verification

The most topical and biggest concern that our survey results highlighted is the ability to effectively age verify all individuals, not just minors. There is a huge operational burden in getting this right and there are also concerns about the quality of current service providers in this space.

Content Moderation

Our survey participants indicated that while processes are in place, there is a need for continual evolution to address new threats and more sophisticated bad actors.

User Data Protection and Privacy

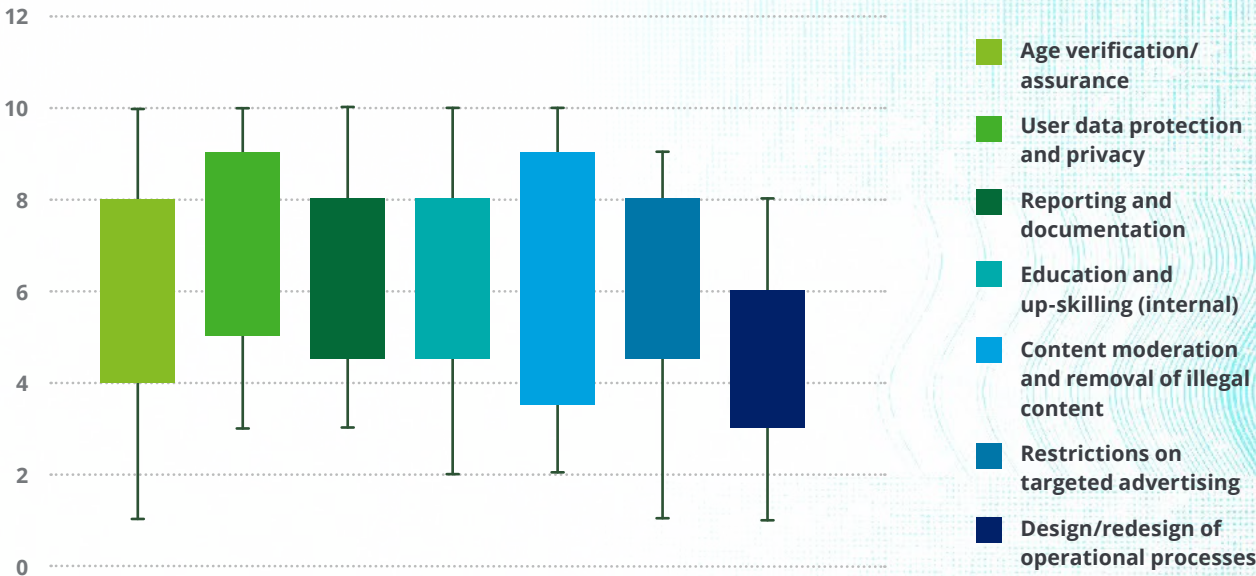
An on-going concern is the lack of trust surrounding how users personal data is processed and the transparency surrounding this. This raises the challenge of repeat and time-consuming requests such as subject access requests and, also, the risk of users losing trust in the product or service.

Targeted Advertising

Inconsistencies in rules and enforcement were flagged where targeted advertising is concerned. There is a perceived imbalance between privacy rights and business freedoms.

Q5. Which of the following regulatory requirements are most challenging for your company?

Rank from 1 (low impact) to 10 (high impact)



NAVIGATING THE CHALLENGES

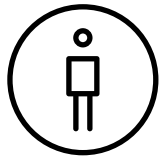
Content moderation and user data protection and privacy are the first and second most challenging requirements, respectively. The nature of the ever-evolving digital landscape means that technology is becoming more and more sophisticated as are bad actors and, the qualification of illegal content is constantly changing. This leads to the fact that it is impossible for any organisation to achieve 100% compliance when it comes to content moderation. Human-centric content moderation throws up challenges of harm to those digesting and policing this content and a move towards utilising AI for content moderation leads to ethical concerns, not to mention potential non-compliance with the AI Act. When we look at user data protection and privacy, it is difficult not to point to going back to basics. Data integrity, transparency and access are the key drivers of consternation amongst users and naturally this leads to challenges around the ability to use data for more targeted advertising.

Age verification is also quickly becoming a major concern and risk to organisations with challenges such as technical immaturity, data protection and cyber risks, not to mention the cost of compliance and implementation. In addition to this, there are concerns around bias in terms of eligible users as well as the ability to navigate age verification technology.

Whilst geo-politics are currently a topic of much debate and concern, signifying a move away from regulation to more of a focus on free speech, this seems to impact mainly the US. In the EU, where the majority of digital regulations police, organisations continue to focus on major compliance changes to address these new requirements. Organisations should ensure that they are educating themselves to the impact of these regulations at global level in addition to:



OUR SUGGESTED APPROACH



Ensuring cross-organisation AI literacy and understanding the prohibitions for AI, particularly where content moderation practices are concerned and the need for human-centricity;



An understanding of all Irish and EU age verification obligations and the risk that exists where age-verification is not effective, implementation of measures proportionate to that risk and with consideration of data privacy and other fundamental human rights; and,



An open dialogue with regulators and lawmakers with the view that the law is evolving in this area and everyone is on the same regulatory journey. It is worth highlighting that whilst age-verification obligations under the various regulations, such as the Online Safety Code and the DSA, apply to designated VLOPs, smaller online platforms should also be conscious that these obligations may extend to them in the future.



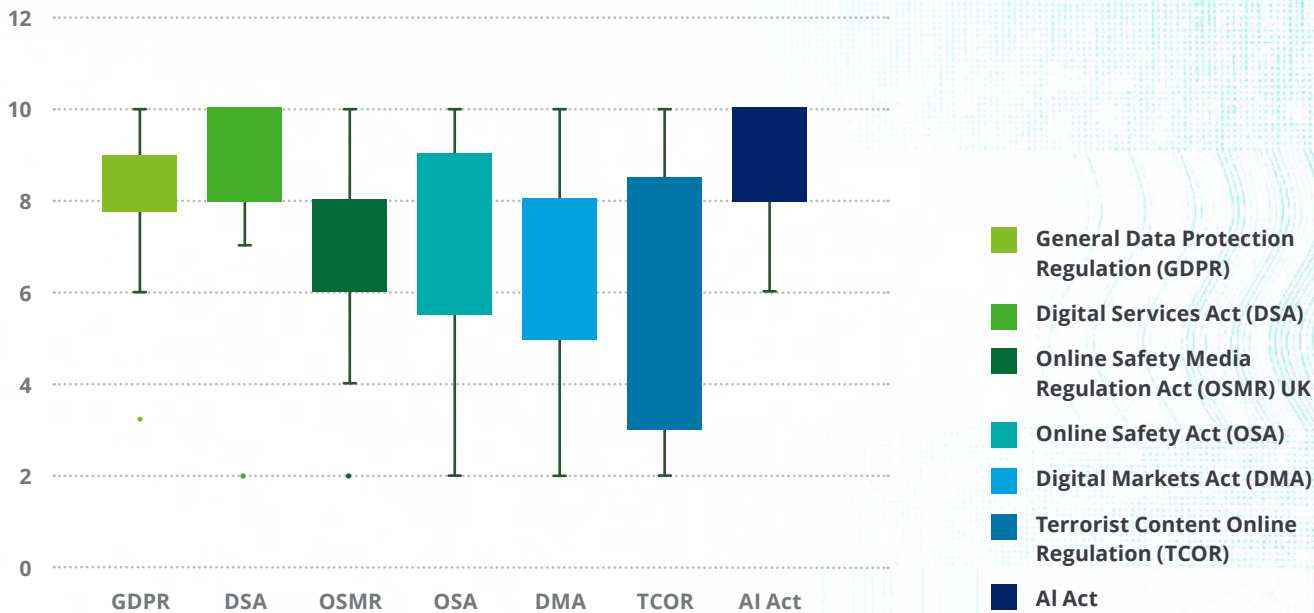
In addition, while ranking low in the survey, education and upskilling as well as efficient reporting and documentation has a huge impact on the various requirements under the regulations and is key to overall compliance.

OPERATIONAL PROCESSES

OPERATIONAL PROCESSES

We asked our survey participants their view on how the various digital regulations will impact operations and, the AI Act, Online Safety Regulations and the GDPR are causing the most concern in terms of high operational burden. Implementing high impact regulations such as these affect time, resources and processes, including on-going design and redesign of frameworks to meet the new requirements.

Q6. To what extent do you believe these online regulations will impact your company's operations
Rank from 1 (low impact) to 10 (high impact)



A NEW WAVE OF REGULATION

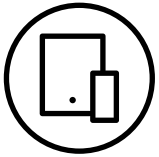
While newer digital regulations are coming out tops in terms of operational burden, there is an advantage to an older regulation such as the GDPR featuring in this response too. The GDPR sets the scene in terms of how to respond to the onerous requirements but also how to stand up a compliance framework from an operational perspective. There have been many lessons learned but a key one has been approaching the GDPR with a 'tick the box' mindset and rolling out policies without adequate operationalisation.

Approaching compliance from the top down and an over-reliance on policy has led to necessary operational re-design and, most significantly, fines for non-compliance.

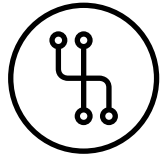
This new and evolving wave of digital regulation is the time for organisations to proactively future-proof in terms of meeting obligations in an operationally effective way:



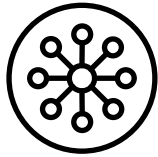
OUR SUGGESTED APPROACH



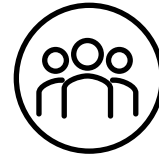
Understand the existing operational effectiveness for existing and emerging digital regulations and consider this in the context of the entire lifecycle from compliance to products and operations;



Join the dots on any siloed or fragmented approach to ensure consistency and efficiency and avoid any duplication of efforts as well as bridging any gap between compliance and operations;



In order to minimise the impact of the regulations, it is becoming increasingly important to understand the links, overlaps and perceived contradictions between regulations and to develop integrated compliance and operational solutions; and,



Consider the operational effectiveness of a Digital Trust function that provides a holistic approach and ensures all key stakeholders (e.g. DPOs, CDOs, CIOs, CISOs) are involved from the beginning.

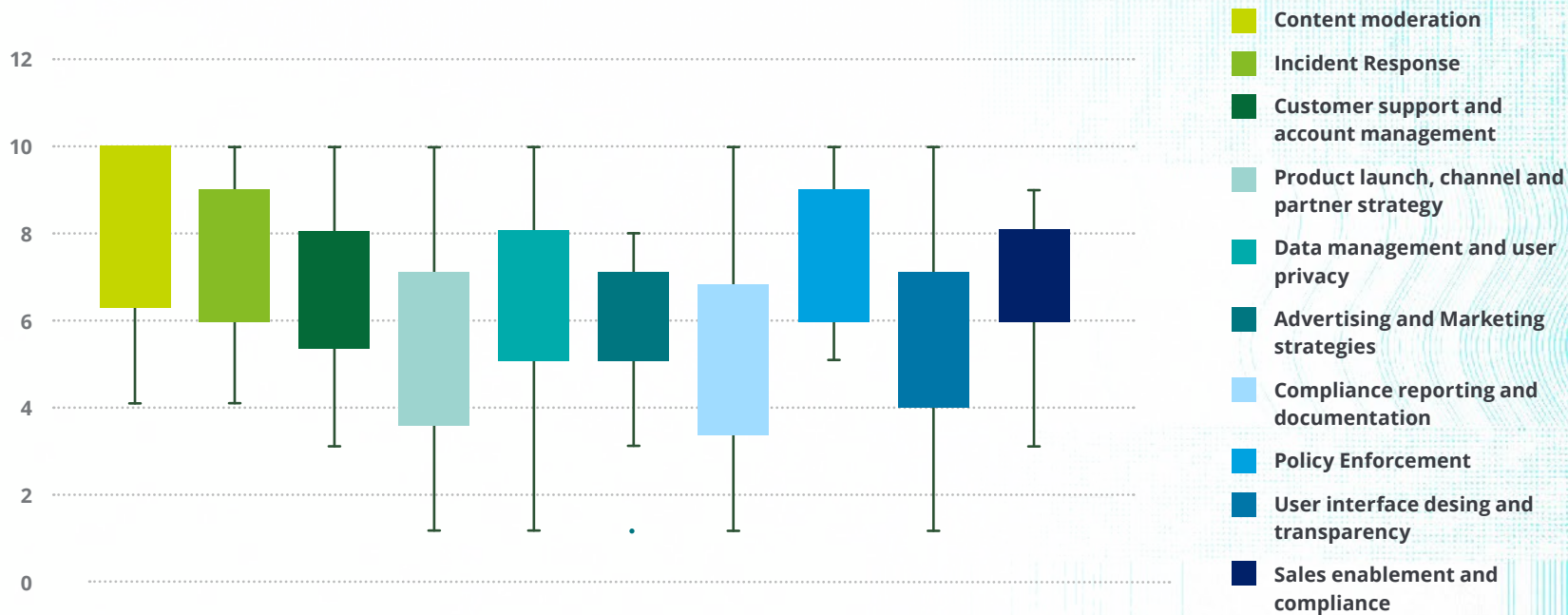
It is important to also highlight data governance practices when addressing any existing or new digital regulation that relies on multiple data sets. A less than effective data governance model is resulting in data being used without essential guardrails which is now leading to compliance and operational issues with GDPR, the DSA and the AI Act. Core components are understanding all existing data sets including unstructured and metadata, ensuring data quality and integrity, data security, data architecture processes and data integration and interoperability. Standards, policies and procedures are key here but beyond that a holistic approach is also fundamental to integrating data governance and data management.

COMMERCIAL IMPACT

COMMERCIAL IMPACT

Content moderation, data management, user privacy and compliance reporting and documentation all featured high in our survey responses in terms of impact. However, our survey participants also expressed concern of impact to product launches, marketing strategies, UI design and sales enablement.

Q7. Which operational processes in your company are (or will be) most impacted by online regulations?
Rank from 1 (low impact) to 10 (high impact)



COMPLIANCE AS AN ENABLER

We already have an understanding that data management, content moderation and compliance reporting are critical areas when it comes to meeting the obligations under the digital regulations. These areas will require a substantial lift in terms of effort, risk assessments, as well as design and re-design of operations. However, there is also a concern and significant challenge connected to the commercial impact that will naturally flow from this. There is a current modus operandi where compliance checks still feature as the last step for any kind of product or service launch and marketing and advertising campaign . This is creating delays in launching and go-to-market strategies and causing frustration and loss of revenue and even the risk of enforcement and fines. There is also a risk that all product

testing will sit outside the EU due to slower and more laboured processes that exist currently. The key is not to rely on last minute check boxes and understanding that these digital regulations require compliance and risk input from proof of concept right through to testing, product launch or any subsequent iterations and enhancements.

Here, a holistic compliance framework is paramount to an effective future-proofed approach. A holistic framework will consider obligations and requirements from emerging regulations as well as support innovation and enablement of new technologies. To move to a compliance as an enabler approach, organisations need to:



INNOVATIVE COMPLIANCE



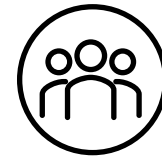
Fully understand the aim and direction of the existing and emerging regulations. Specifically, the fact that compliance approaches need to be much closer to the systems, products and technology;



Lead with a Trust by Design framework, ensuring that safety, integrity, accessibility, security, privacy and transparency are baked into the technology from the outset and risk is addressed throughout the lifecycle. For digital regulations, this means a move away from the status quo of layering on compliance. We are in a new era of regulation when it comes to the digital world where traditional frameworks will not work in the same way and will impede innovation. There needs to be a clear delineation between a proactive digital compliance framework and the legal teams, whose job is to defend and therefore be reactive;



Consider budget for the end-to-end product launch or market strategy. Non-compliance will only result in losing opportunities, delayed product launches, loss of revenue and potential fines; and



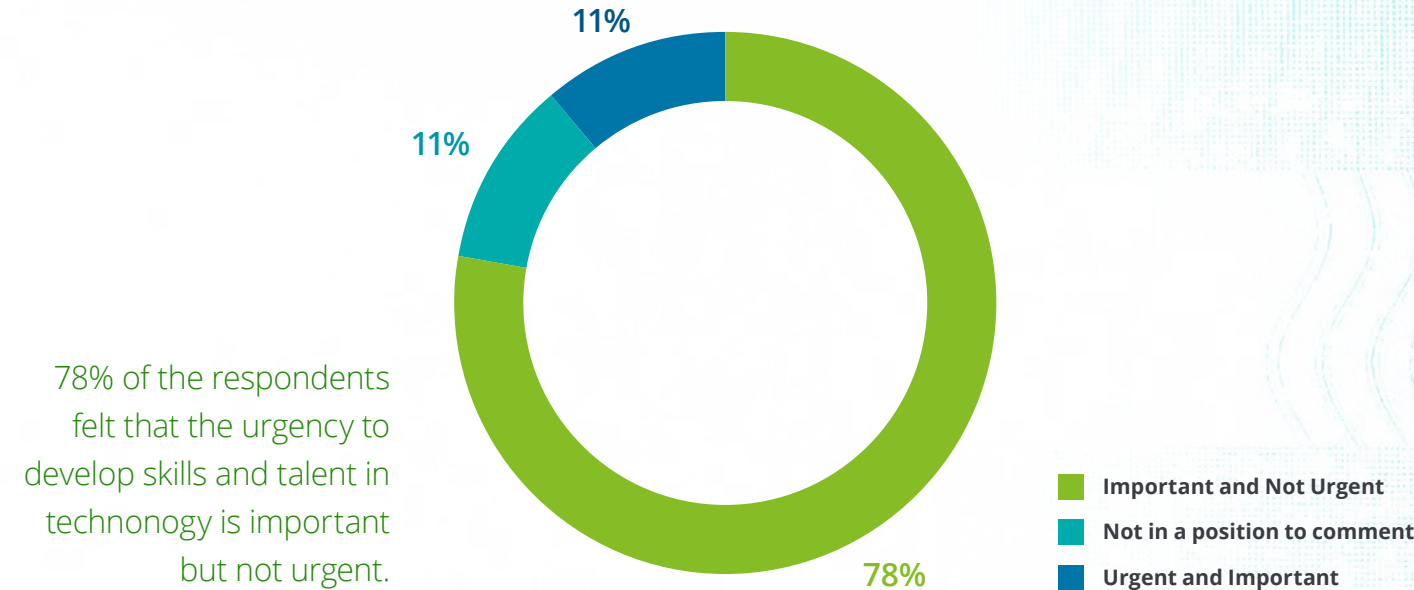
A strong and strategic business case will be important with input from all relevant stakeholders (DPO, CPO, CRO, CISO, CDO, CIO etc.)

TALENT, LITERACY, EDUCATION

TALENT, LITERACY, EDUCATION

One of the more surprising results of our survey is that 78% of the respondents felt that development of skills and talent in technology is important but not urgent.

Q9. How would you rate the urgency and importance to develop skills and talent within your organisation today to face these regulatory demands?
Urgency and Importance to Develop Skills and Talent



EDUCATION IS NECESSARY TO PROGRESS

One of the most important lessons learned from the implementation of the GDPR right through to today is that continuous education across the organisation is a necessity. The lack of education at the implementation phase has resulted in many organisations now re-designing their approach to data privacy across the three lines of defence. Lack of knowledge, skills and talent in the right places has resulted in enforcement orders and fines and a retroactive effort to understand risk across the business. We also see that on the 2nd February 2025, one of the first requirements of the AI Act to come into force, Article 4, deals specifically with AI

literacy and an indication that there needs to be training and development relative to the proposed AI and sufficient level of understanding of the risk. Lack of adequate training for digital regulations will result in knowledge gaps, leading to fragmented and siloed approaches to risk and compliance. This will result in unsuccessful or delayed products/new technologies and enforcement orders, fines and mitigation. What follows from this is the absorption of resources into reactive mitigation measures, revenue loss and ultimately customer/consumer trust.



NEXT STEPS

Organisations should ensure that:



They quickly stand up an education programme across the 3 lines of defence to ensure that there is an adequate level of understanding relative to the specific regulation and that there is continuous upskilling to keep pace with the regulatory changes as well as the technology changes;



The right talent and skillsets exist within all areas of the business;



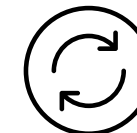
They support and, engage in, knowledge sharing through industry groups, peer interactions and events;



There is more open and continuous dialogue and proactive engagement with the relevant Regulators. Not only will this support compliance efforts but the proximity in Ireland with these Regulators allows for more frequent and effective communication, ensuring alignment with expectations and ability to address compliance efforts proactively. This engagement also works both ways and will not only guide organisations in the right direction but also the Regulators themselves. Educating the Regulators on the challenges organisations face and the nuances within different technologies is key;



They are undergoing research now to understand what types of tooling exists to support identification and oversight of compliance and create efficiencies and harmonies across the digital regulations with a customer centricity approach; and



Ultimately, they are keeping pace and engaging with all regulatory developments in this digital space, including paving the way for a more predictable and stable regulatory environment. This is crucial for continued investment and to support innovation.

CLOSING STATEMENT

This next year will test the mettle and fabric of every big tech player in Europe. As digital regulations such as the AI Act, DMA, DSA and OSC bite, and the GDPR becomes even more relevant, the patient nudge of principle is giving way fast to the vigorous enforcement of watertight regulation.

For sure, navigating these waters needs expert help in interpreting these complex regulations. But interpretation is just step one. From operations to risk and human capital to marketing, organisations need to urgently stand up the machinery of living, futureproof compliance. Growing regulatory dissonance with other regions makes this more and more a local problem to solve, at the heart of the EU regulatory landscape.

We are already working closely with countless affected organisations. We are already designing and delivering end-to-end readiness. We are

already confidently sailing these uncharted waters.

Vitality, we have a close and constructive relationship with the regulators and we share their mission, to help organisations create and maintain sustainable and transparent end-to-end compliance.

Deloitte Ireland knows that landscape inside out and, is uniquely positioned to help our clients succeed in this changing world.

We are ready to partner with organisations and lead together to protect society, gain customer trust, and enhance innovation at the highest level, making Ireland, already a digital hub, a digital hub for the future.

We would like to thank survey participants for their honest and insightful responses to our survey.



GET IN TOUCH



Nicola Flannery

Partner, Digital Trust & Privacy Lead



Ciaran McGovern

Partner, TMT



Colm McDonnell

Partner, Head of Technology, Media & Telecoms Industry





At Deloitte, we make an impact that matters for our clients, our people, our profession, and in the wider society by delivering the solutions and insights they need to address their most complex business challenges. As the largest global professional services and consulting network, with over 450,000 professionals in more than 150 countries, we bring world-class capabilities and high-quality services to our clients.

In Ireland, Deloitte has over 3,000 people providing audit, tax, consulting, financial advisory, and risk advisory services to public and private clients spanning multiple industries. Our people have the leadership capabilities, experience and insight to collaborate with clients taking them wherever they want to go.

This document has been prepared by Deloitte Ireland LLP for the sole purpose of enabling the parties to whom it is addressed to evaluate the capabilities of Deloitte Ireland LLP to supply the proposed services.

This document is not an offer and is not intended to be contractually binding. Should this proposal be acceptable to you, and following the conclusion of our internal acceptance procedures, we would be pleased to discuss terms and conditions with you prior to our appointment and no reliance may be placed for any purposes whatsoever on the contents of this document.

Deloitte Ireland LLP is a limited liability partnership registered in Northern Ireland with registered number NC001499 and its registered office at The Ewart, 3 Bedford Square, Belfast, BT2 7EP, Northern Ireland.

Deloitte Ireland LLP is the Ireland affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

The Deloitte Ireland LLP privacy notice is available at www.deloitte.ie/privacy

© 2025 Deloitte Ireland LLP. All rights reserved.