Novacoast

GENERAL DATA PROTECTION REGULATION OVERVIEW

Mick Tennent
Director Security Services

General Data Protection Regulation

KEY POINTS

The General Data Protection Regulation

After four years of negotiation the General Data Protection Regulation (GDPR) came into effect on 25th May 2018. This new law introduced a range of requirements that has significant impacts on organisations. Combined with increasing demand from consumers, privacy is now firmly positioned at the top of EU corporate agendas.

Conformity and Enforcement

For Global organisations, GDPR provides conformity of the old fragmented legal frameworks of Privacy across Europe, providing a single data protection regulation for all member states. While the regulations have been harmonised, GDPR introduces a new maximum monetary penalty of 4% annual global turnover that can be imposed in cases of serious non-compliance.

New Requirements

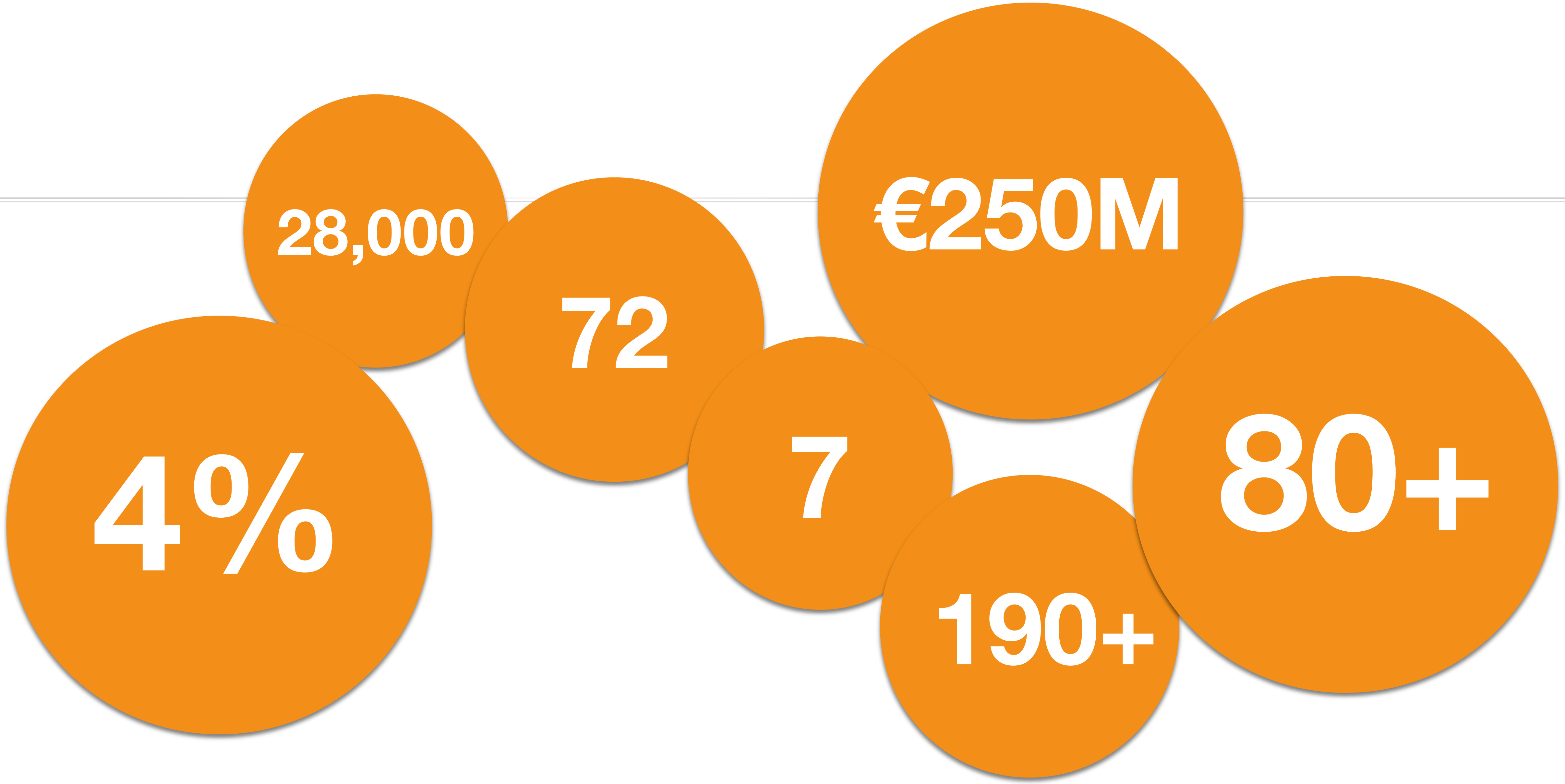
GDPR mandates organisations are accountable and will be required to implement robust privacy governance and in general take a more proactive approach to privacy compliance. Documented privacy risk assessments will be required for new systems and technology. Data breaches will be notified to regulators within 72 hours.

International Reach

Organisations based outside of the European Union (EU) that process data to offer goods or services to European residents, or to monitor the behaviour of European residents will also be subject to GDPR requirements. How enforcement will apply in practice is yet to be seen, but organisations that previously were not in scope of EU data protection rules as per individual member states, may find themselves subject to significant new requirements.

General Data Protection Regulation

SOME NUMBERS



28,000

72

4%

7

€250M

190+

80+

General Data Protection Regulation

GDPR FINE EXAMPLES - NOT CURRENTLY ENFORCED

€1BN

BRITISH AIRWAYS

6%

€720M

UBER

The Key Changes of the GDPR

Fines of up to 4% of annual global turnover

€'000 → €'000,000

Previously fines were limited in size and impact. GDPR fines will apply to both controllers and processors.

Increased territorial scope

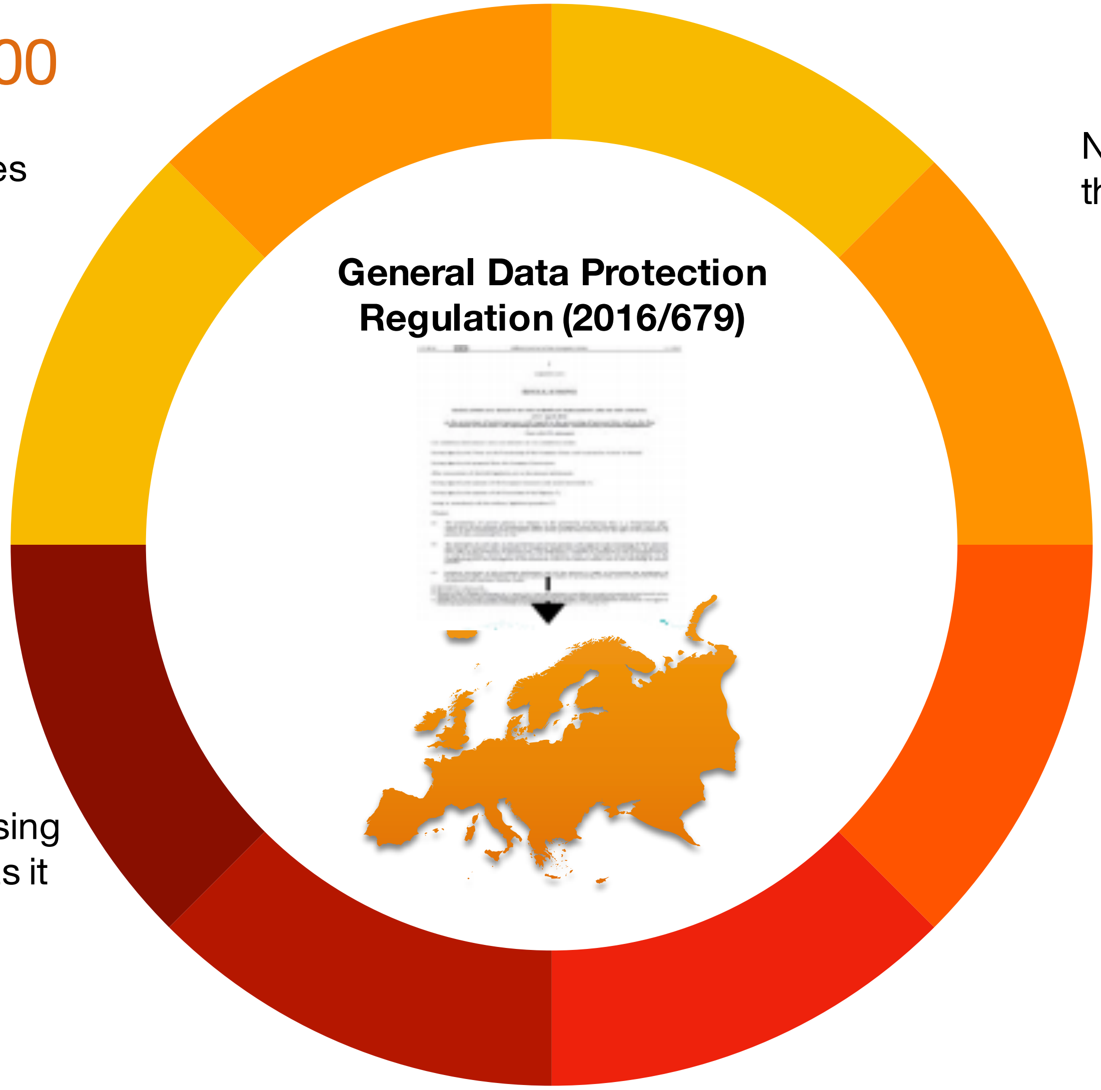
GDPR will apply to all companies processing the personal data of data subjects residing in the EU, regardless of the company's location.

Explicit and retractable consent

Must be provided in an intelligible and easily accessible form, using clear and plain language. It must be easy to withdraw consent as it is to give it.

Right to access and portability

Data subjects can request confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format.



General Data Protection Regulation (2016/679)

Breach notification within 72 hours

Now mandatory that breaches, which are likely to "result in a risk for the rights and freedoms of individuals", are reported within 72 hours of first having become aware of the breach.

Privacy by design

Now a legal requirement for the inclusion of data protection from the onset of the designing of systems, rather than in retrospective addition.

Right to be forgotten

Entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data and potentially have third parties halt processing of the data.

Mandatory data protection officers

Appointed in certain (public authorities, when monitoring of data subjects on a large scale and when processing special categories of data). To facilitate the need for a company to demonstrate their compliance to the GDPR and compensate for GDPR no longer requiring the bureaucratic submission of the notifications/registrations of data processing activities or transfers based on Model Contract Clauses.

General Data Protection Regulation

KEY POINTS

Legal and Compliance Perspective

GDPR introduces significant new requirements and challenges for legal and compliance functions. Organisations will need to put in place additional governance and controls.

Technical and Digital Perspective

New GDPR requirements will mean changes to the ways in which technologies are designed and managed, including a focus on profiling and security.

Data Perspective

Individuals and teams tasked with data governance and data management will be challenged to provide clearer, proactive oversight on data storage and journeys.

Let's put some perspective on Legal and Compliance

Revolution in Enforcement

Fines of up to 4% of annual global turnover

Serious non-compliance could result in fines of up to 4% of annual global turnover, or €20 million - whichever is higher. Enforcement action will extend to countries outside of the EU, where analysis on EU citizens is performed. But how will this play out in practice?

Accountability

Burden of proof now on the organisation, not the individual

The current requirement to provide annual notifications of processing activities to local regulators will be replaced by significant new requirements around maintenance of audit trails and data journeys. The focus is on organisations having a more proactive, comprehensive view of their data and being able to demonstrate they are compliant with the GDPR requirements.

Data Protection Officers

Market hots up for independent specialists

Organisations processing personal data on a large scale will now be required to appoint an independent, adequately qualified Data Protection Officer. This will present a challenge for many medium to large organisations, as individuals with sought-after skills and experience are currently in short supply. Organisations will also be challenged to demonstrate an independent reporting line, which could cause issues with incumbent positions.

Privacy notices and consent

Clarity and education is key

Organisations will now consider carefully how they construct their public-facing privacy policies to provide more detailed information. However, it will no longer be good enough to hide behind pages of legalese. In addition, there is a significant shift in the role of consent, with organisations required to obtain 'freely given, specific, informed and unambiguous' consent, while being able to demonstrate these criteria have been met.

Let’s put some perspective on Technology

Breach reporting within 72 hours of detection

Significant data breaches will now have to be reported to regulators and in some circumstances also to the individuals impacted. This means organisations will have to urgently revise their incident management procedures and consider processes for regular testing, assessing and evaluating their end to end incident management processes.

Breach reporting

Online Profiling

Profiling becomes a loaded topic

Individuals will have new rights to opt out of and object to online profiling and tracking, significantly impacting direct to consumer businesses who rely on such techniques to better understand their customers. This applies to not just websites, but also other digital assets, such as mobile apps, wearable devices and emerging technologies.

Encryption as means of providing immunity?

The GDPR formally recognises the privacy benefits of encryption, including an exemption from notifying individuals of data breaches when data is encrypted. However, this does not mean that organisations can afford to be complacent and the exemption may not apply when weak encryption is used. Given the potential fines, organisations will have to further increase their focus on a robust information and cyber security regime.

Encryption

Privacy-by-design

Recognised best practice becomes law

The concept of Privacy By Design (PbD) is nothing new, but now it is enshrined in GDPR. Organisations need to build a mindset that has privacy at the forefront of the design, build and deployment of new technologies. One manifestation of PbD is Data Protection Impact Assessments (DPIA), which are now required to be undertaken for new uses of personal data where the risk to individuals is high.

Let’s put some perspective on Data

Data Inventories

Identifying and tracking data

Organisations will have to take steps to demonstrate they know what data they hold, where it is stored and who it is shared with, by creating and maintaining an inventory of data processing activities. Data leads will have to work closely with privacy colleagues to ensure all necessary bases are covered. A thorough system for maintaining inventories needs to be created.

Right to data portability

A new right to request standardised copies of data

A new right to ‘data portability’ means that individuals are entitled to request copies of their data in a readable and standardised format. The interpretation of this requirement is debatable, but taken broadly the challenges could be numerous - amongst them achieving clarity on which data needs to be provided, extracting data efficiency and providing data in an industry-standardised format.

Right to be forgotten

A stronger right for consumers to request deletion of their data

A new ‘right to be forgotten’ is further evidence of the consumer being in the driving seat when it comes to the use of their data. Depending on regulatory interpretation, organisations may need to perform wholesale reviews of processes, system architecture and third party data access controls. In addition, archive media may also need to be reviewed and data deleted.

New definitions of data

New concept of pseudo-anonymous data

The GDPR recognises the concept of pseudo-anonymous data and at the same time expands the definition of personal data, placing a greater emphasis on data classification and governance. It remains unclear if and when certain data, for example IP addresses, will be classed as personal data and subject requirements.

Implementing GDPR

Considerations for Implementing GDPR

Executive Sponsorship, business accountability and multi-disciplinary approach

- Senior visibility and sponsorship is key. GDPR touches all aspects of an organisation's operations and you will require the right support to drive organisational changes that are required.
- This is not just an IT or Legal problem. Business, system and data owners all need to be made accountable for how they handle personal data for the required changed to become embedded.
- A wide range of stakeholder engagement is required. There are few compliance topics that have implications across a wide range of areas, including customer engagement, marketing, security, personnel management and technology.

Target state definition and outcome-based approach

- In many programmes we see a disconnect between the programme team and the business, each looking at each other for increased guidance or ownership. A clear and agreed state across each GDPR area is required to bridge this gap.
- Important to drive towards collective outcomes; this may in some cases that the programme team allows the business to implement certain requirements, ensuring there is consistency, for example consent and marketing.

Risk appetite and risk-based approach

- The Regulation encourages a risk-based approach. This can be applied across many aspects; from completeness of your data inventory, to which systems you proactively analyse and prepare so they can deal with rights, such as portability and erasure.
- Initially setting out the risk appetite is difficult but important task; is your goal to just gain compliance, or for privacy to be a strategic initiative?

Targeted internal messaging - see the benefits

- GDPR may well be down the list of many people you engage with and whose support you need. It is vital to ensure internal messaging is relevant such that everyone can see the importance of the topic. This involves understanding their individual role, the impact of getting it wrong and the benefits that a proactive approach to privacy can bring in terms of customer trust and engagement.

Operating model - think long term

- This is not something that is going away anytime soon. Make sure your programme includes the definition of a long term operating model that sets out roles and responsibilities such as how privacy risk is managed and how it was monitored and assessed.
- This should include the role of enabling technology as the programme matures; where efficiencies can be gained rather than knee-jerk technology purchases.

Actions to take to prepare for GDPR

GDPR READINESS ASSESSMENT

GDPR TRANSFORMATION PROGRAM

DATA PROCESSING INVENTORY

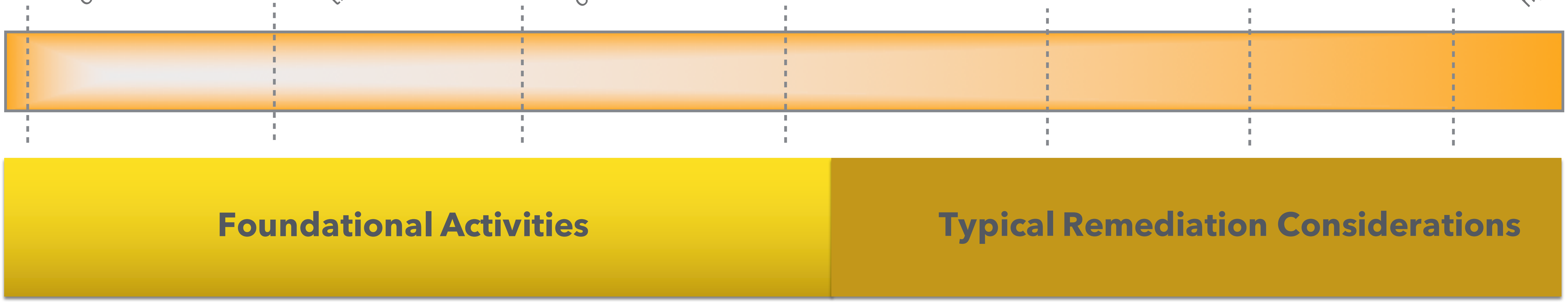
PRIVACY BY DESIGN

THIRD PARTY PROCEDURES

Key Activities and Considerations

TO REACH GDPR COMPLIANCE BOTH FOUNDATIONAL AND REMEDIAL ACTIVITIES ARE REQUIRED

- **Stakeholder Awareness** Ensure key stakeholders are fully aware of the GDPR and the impact it will have on the organisation
- **Readiness Assessment** Conduct a readiness assessment to understand how near or far away the organisation is from the relevant new requirements
- **Data Inventories and Mapping** Compile an inventory of the personal data collected, who it is shared with and what controls govern its use
- **Governance** Use the GDPR to assess the holistic approach to privacy - how is data protection governed and what are the roles and responsibilities?
- **Legal and Compliance** Determine how compliance will be demonstrated, review approaches to capturing consent and re-draft privacy notices
- **Technology** Deploy technology and processes to bring about a Privacy by Design culture
- **Data** Ensure the organisation has the right data governance practices to respond efficiently to the new rights afforded to individuals



Foundational Activities

Typical Remediation Considerations

GDPR Readiness Assessment

The road to GDPR compliance with a readiness assessment

What is a GDPR Readiness Assessment

To give a clear picture on where your organisation currently stands with respect to the GDPR. The Readiness Assessment is:

- A tool to create a baseline of privacy;
- Potential to incorporate into your broader Cyber strategy and roadmap;
- A good starting point for becoming compliant with the GDPR and getting a tailored privacy program;
- Based upon Privacy, Security and Governance framework, covering all elements of the described privacy program;
- Instrumental in finding areas of biggest risk;
- Used to focus on those areas which most urgently need action to become GDPR compliant;
- A method to measure how mature the organisation currently is, using known privacy and data protection maturity models.

1. Capture Business Requirements

Privacy compliance and GDPR Readiness framework tailored based on industry and organisational characteristics

2. Insight into Current Privacy Situation

A thorough assessment by workshops and interviews with parts of the organisation, giving insight of the current level of maturity against the framework

3. Develop Strategy & Roadmap

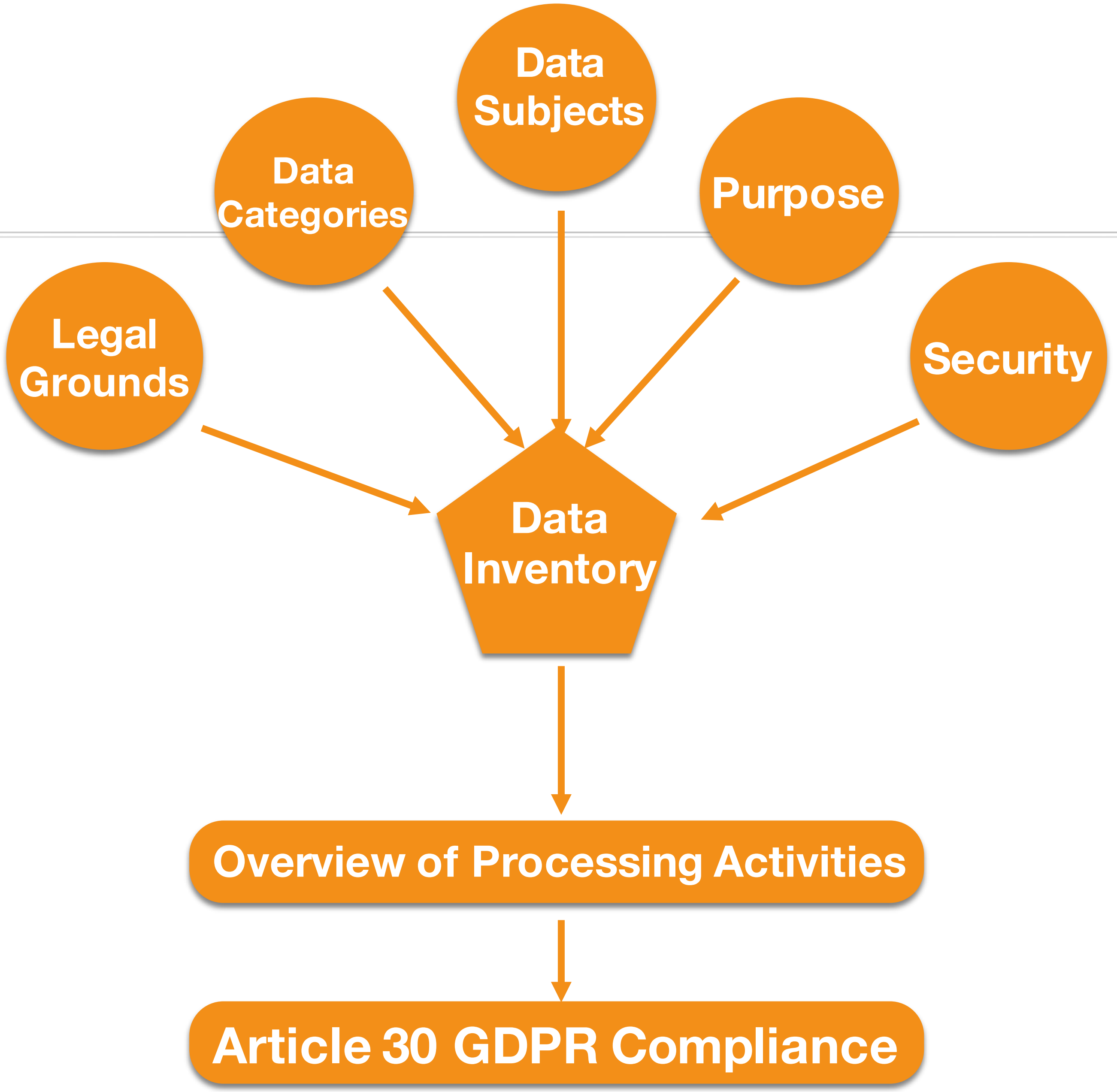
A practical and concrete roadmap with prioritised steps required to improve, risk-based and state of privacy compliance with GDPR

Data Processing Inventory

Creating a data Inventory provides an overview of all data and insight in the risks attached to processing activities

A Data Processing Inventory is your basis to get control of your data processing

- A data inventory is an overview which includes all the required information concerning personal data processing, such as legal grounds, purpose, categories of data, retention period and conducted risk analysis.
- Having an inventory is an actual requirement under the GDPR (article 30), but it can also serve you well in building your understanding of the personal data you process.
- The inventory is used as a register of all the data processes within the organisation. Having an inventory is essential for your oversight of processing activities and is a mandatory element of GDPR compliance.
- The inventory allows your organisation to demonstrate awareness of its obligations as a data controller, including keeping of records of processing activities.
- Finally, knowing which personal data the organisation processes mitigates the risk of unidentified data breaches.



Privacy by Design

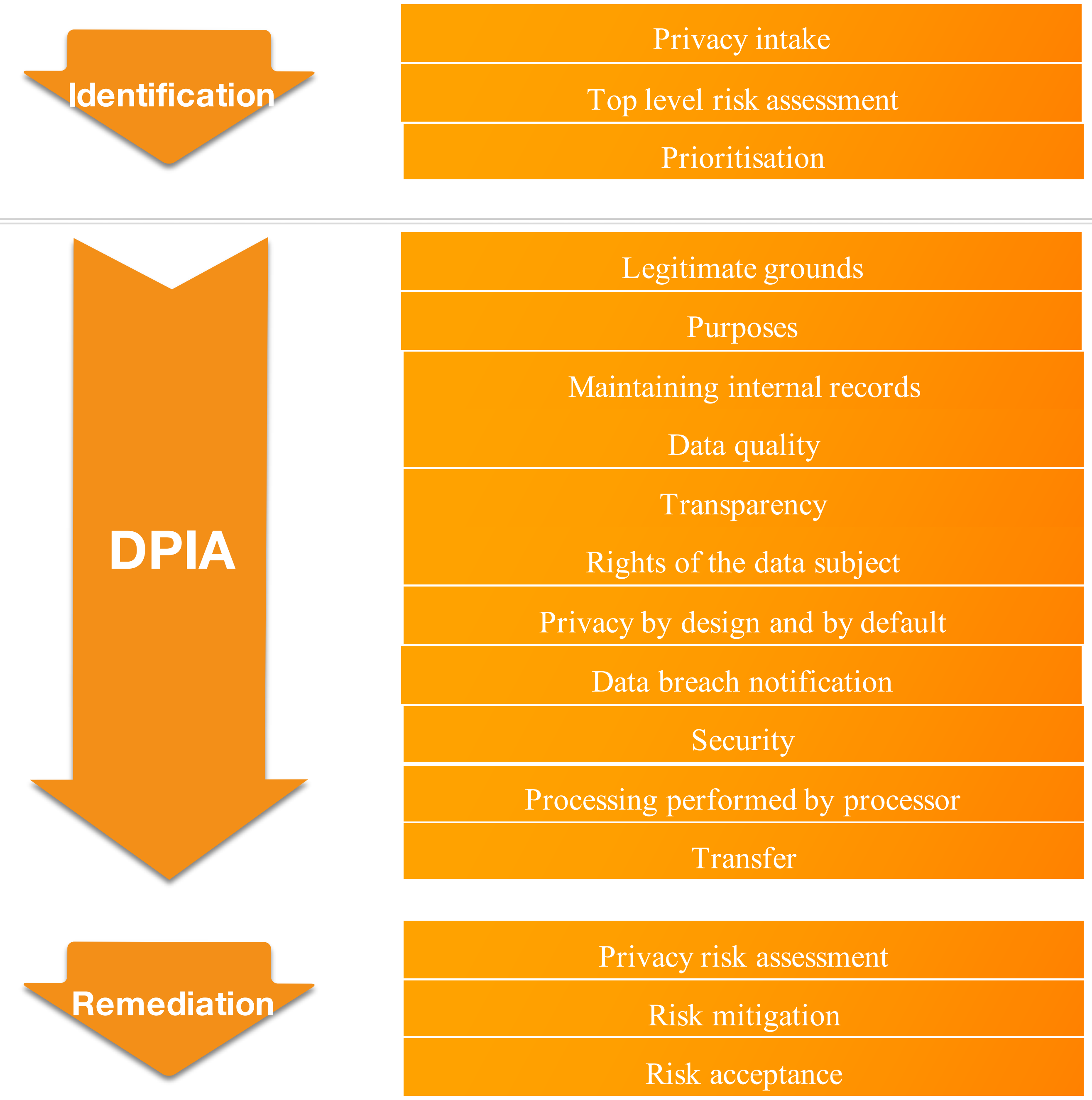
Embedding privacy into your project methodology by assessing risk at an early stage

A tailored approach

Privacy can be considered as an operational risk that requires practical solutions in order to make sure that risk is actually handled. The challenge is to provide uniform and flexible methodologies and progress to safeguard privacy every time a data driven project starts.

Key elements to consider

- Ensuring new projects abide by the privacy rules within your organisation is done through a Privacy by Design approach;
- Data Protection Impact Assessments (DPIA) are based on the GDPR and are a proven and effective tool to assess privacy risks;
- A Privacy by Design approach consists of a number of elements: a PbD process, DPIA method and a remediation framework:
  - The DPIA process describes the phases of identification, DPIA and remediation covering roles, responsibilities, sign offs, escalation, support for a DPIA and should be efficient and effective;
  - The DPIA method is the combination of checks, questions and requirements to assess the impact and risks that any system or project should follow;
  - Remediation should always be the end phase and makes sure impact is reduced and risks mitigated or accepted.



Identification

Privacy intake

Top level risk assessment

Prioritisation

DPIA

Legitimate grounds

Purposes

Maintaining internal records
Data quality

Transparency
Rights of the data subject

Privacy by design and by default

Data breach notification

Security

Processing performed by processor

Transfer

Remediation

Privacy risk assessment

Risk mitigation

Risk acceptance

Third Party Procedures

External parties bring specific challenges for data controllers

When a data breach occurs there are many internal and external challenges. Handling and communication procedures with processors, authorities and data subjects are essential for effective data breach handling.

Data breach handling procedures

Data processing agreements (DPA)

Are your DPAs GDPR proof? With the new data breach rules in place there is a requirement for contractual arrangements between Controllers and Processors.

Every time your organisation uses a third party for any kind of service that might involve data processing there should be a concrete process with clear requirements to assess these parties and their specific service.

To make sure this is done effectively there needs to be collaboration between legal, risk, IT and procurement with strong steering from the Data Protection Officer (DPO).

VENDOR ASSESSMENT

DATA SUBJECT RIGHTS PROCEDURE

The most important external stakeholder are your data subjects. The GDPR brings increased rights to data subjects (customers, patients, citizens) and this brings procedural challenges to a controller. Whether a data subject requests access, erasure or transfer of their data, a good process on how to communicate and serve these data subjects is essential.

Incident Reporting

Requires all data controllers to report certain types of personal data breaches to the relevant authority. You must do this within 72 hours of becoming aware of the breach where feasible.

Situational Analysis

Tell the supervisory authority as much as you can about what happened, what went wrong and how it happened.

Few organisations really understand whether they are ready to respond to an incident. When disaster strikes, the clock starts ticking. Are you ready to respond to a breach?

Assessing the affected data

What categories of personal data have been affected and how many records?

Not knowing what personal data you hold or where and how it is stored is a barrier to assessing the scope and impact of a data breach.

Describing the impact: Potential Impact

Please describe the possible impact on data subjects as a result of the breach.

Establishing the impact of a breach and the extent of the damage caused can be difficult of even a seasoned information security expert.

Reporting on staff training and awareness

If a staff member was involved in the breach, had they received data protection training in the past two years?

Do your staff know how to determine whether a breach has occurred and the appropriate steps to respond to the incident?

Preventative measures and taking action

Describe the actions you have taken, or propose to take as a result of the breach.

Without a comprehensive security programme, any technology will fall short of providing adequate protection

Oversight

The data protection officer, or the senior person responsible for data protection in your organisation.

Many organisations, may find that the DPO responsibilities are a challenge to deliver, given the breadth of knowledge required.

The effect of Brexit for UK Organisations

Extra-territorial Reach

Organisations offering goods or services within the EU, or monitoring the behaviour of EU citizens, will still have to comply with GDPR rules.

UK Data Protection Rules

UK adopted GDPR but an update to the Data Protection legislation seems inevitable. Any UK successor legislation will likely have to deal with similar requirements, in view of the UK's likely intention to apply for 'adequacy status'.

Regulation Enforcement

It has yet to be determined if UK regulatory authorities, post Brexit, can or will apply the same level of punitive measure that GDPR has introduced. The European Commission has not indicated that it will expect to see a comparative framework in countries seeking an equivalent level of data protection standards.

Supply Chain Management

Existing contractual agreements may exist with suppliers and/of clients regarding the transfer of personal data outside of the EU or European Economic Area (EEA). Organisations in the UK are conducting reviews of such contracts and amending terms where necessary.

Thank you

Novacoast

International Network of

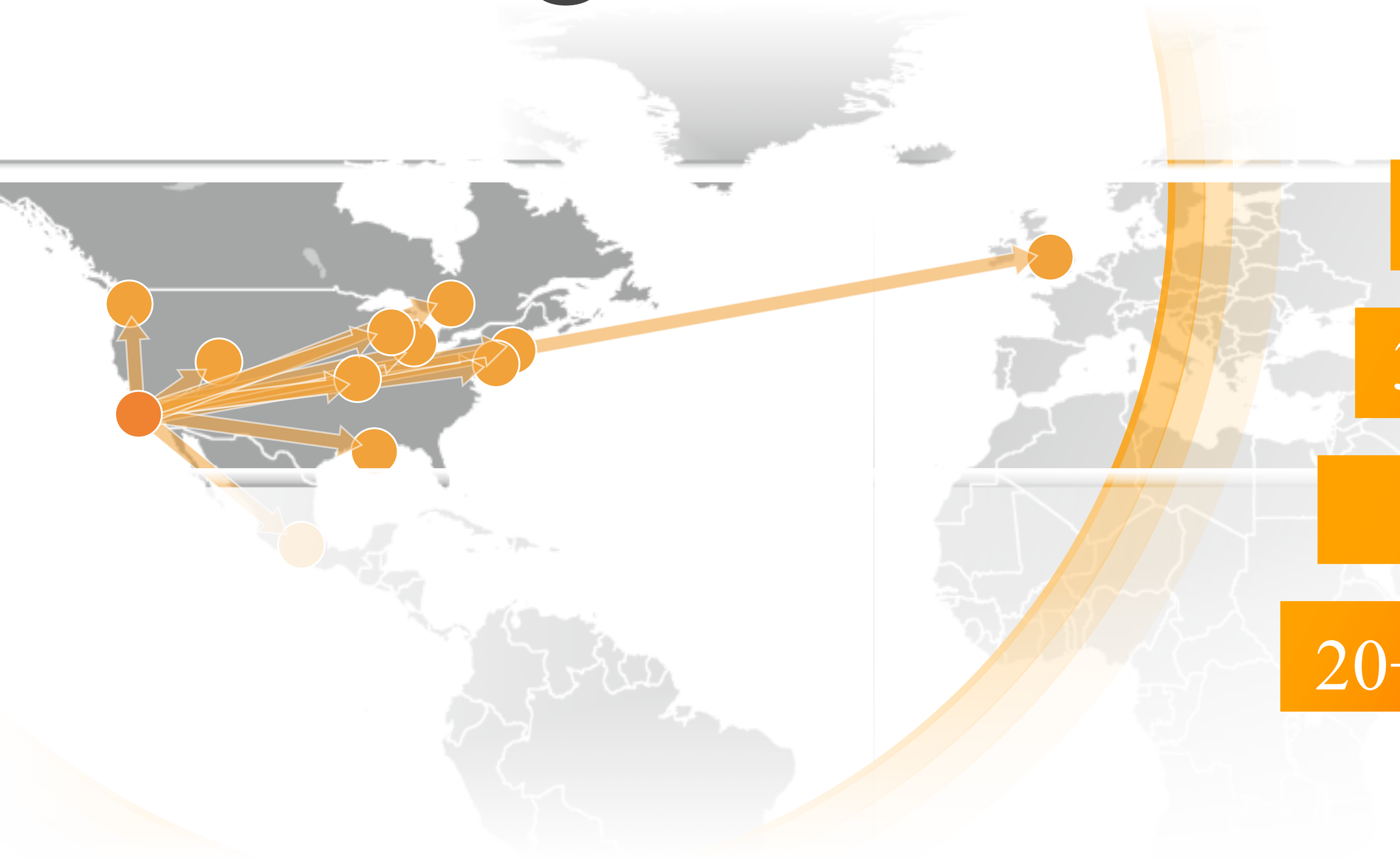
IT Security Resources

Novacoast helps organizations FIND, Create & Implement solutions for a Powerful security posture

through Advisory, Engineering, Development & Managed services.

International Network of

Growing Influencers



Domestic Global

300+ Employees

Vast majority Technical

20+ Years Privately Held

International Network of

Technology Experts

Engineering Services

Cyber Security & Compliance
Assessments, strategy posture improvement, response & compliance

Identity & Access
From Identity to data, endpoints to automated workflows

Development Services

Software Development
Custom software from enterprise to social, native & mobile

Managed Services

Managed Services
Dedicated NOC / SOC departments & Managed IT experience in multiple locations across the world

Supported by

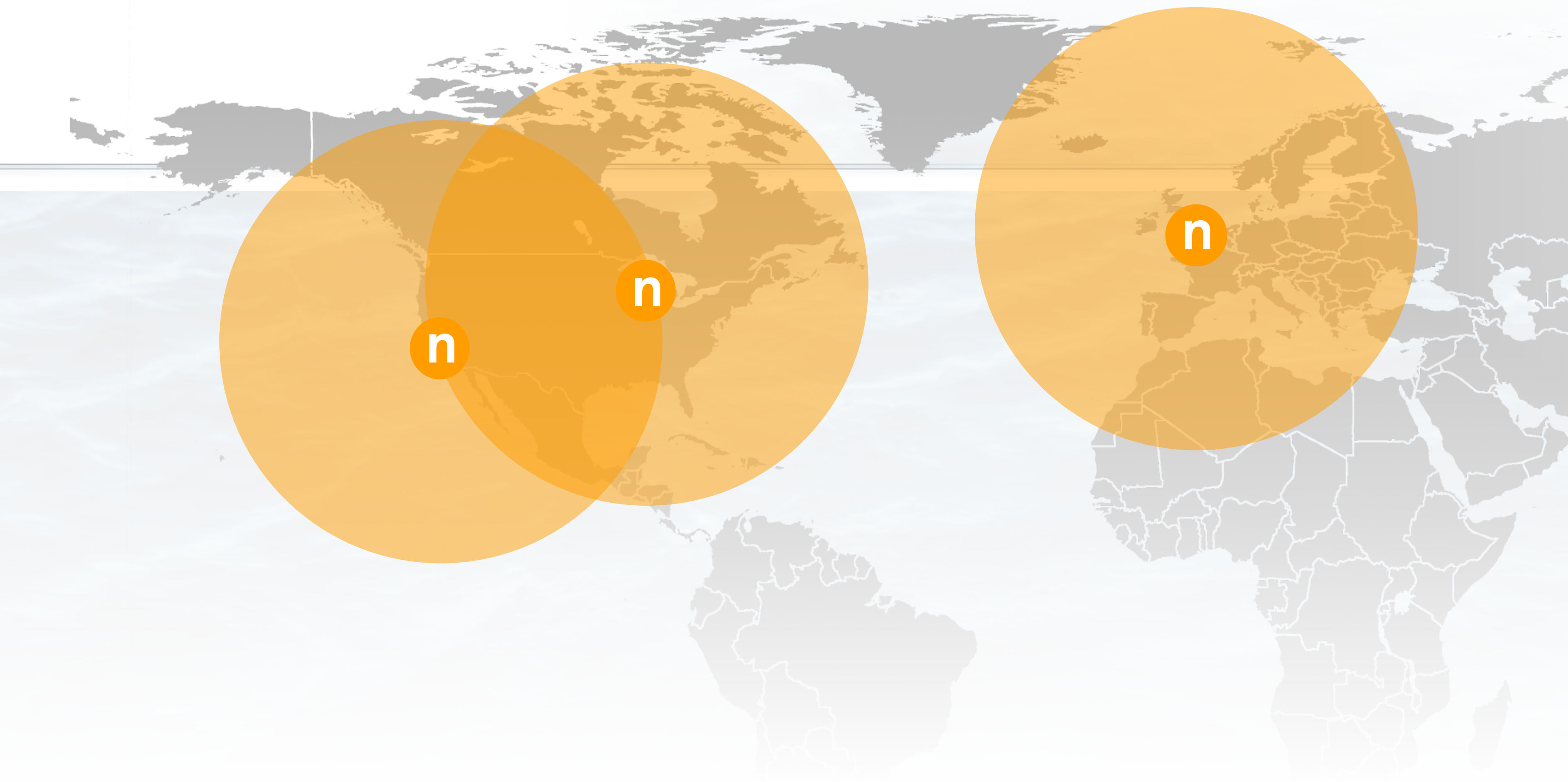
Staffing SERVICES

Training SERVICES

Product FULFILLMENT

International Network of

SOCS



Managed Services

NOC Care, Change Control, Configurations & Uptime

SOC Analysis, Investigation, Escalation, Notification & Reporting

Maturity Assessments, Planning & Improving Security Posture

Engineering Custom Integration, Fixes & Expansions

Leaders in

Integration

Fearless

We'll take it on.
We thrive on difficulty.

Big Picture

A security posture is built piece by piece.
We make it not just work, but work together.

There's a gap between your needs & what is available.
We have the development expertise to close it.

Customization

Long-Term

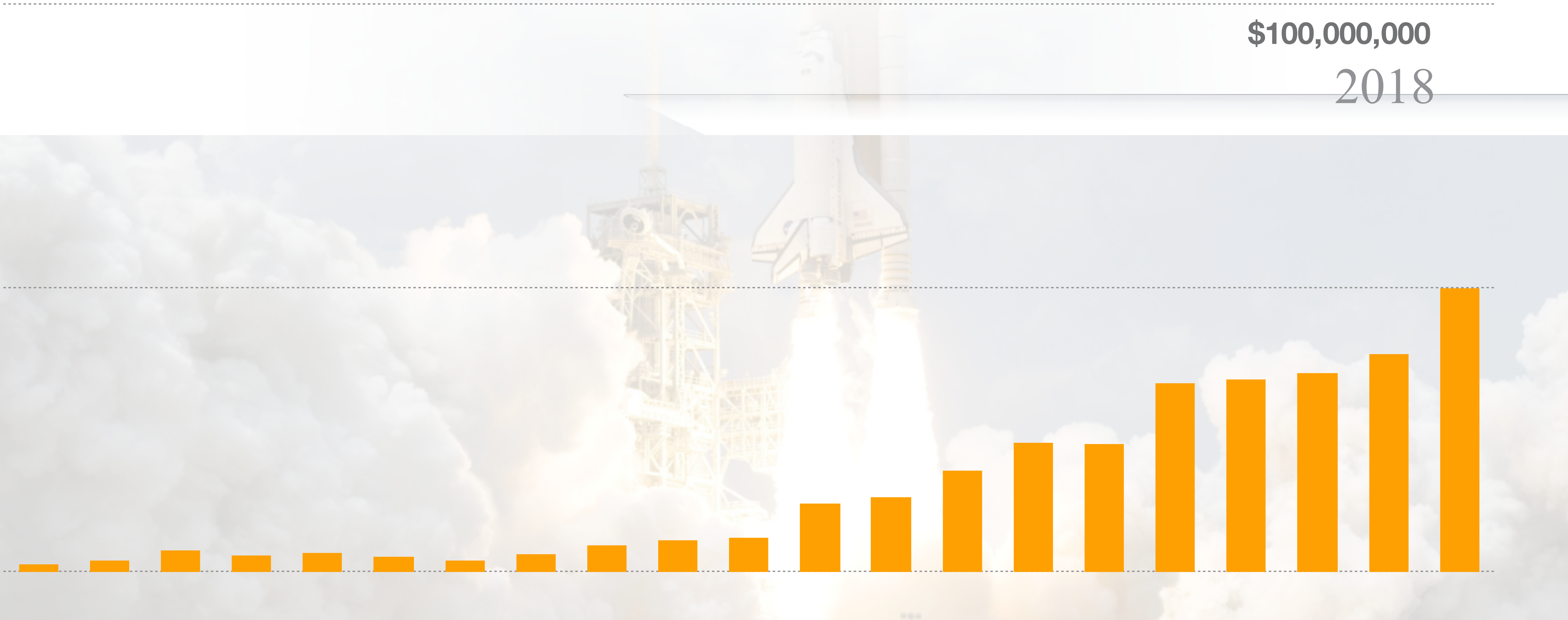
Security is a roadmap, not a snapshot.
We'll plan ahead together.

Your solution may simply not exist.
We can build it from scratch.

Innovation

Decades of

Strong, steady growth


$100,000,000
2018