premex group

OUR GDPR FRAMEWORK

OUR GROUP GDPR INFORMATION SECURITY FRAMEWORK

Continuously improving our information security infrastructure for 2018 and beyond.

MISSION STATEMENT

Governance

Our Group has worked hard to build a governance framework that embodies information security at its heart. This allows us to support our customers in meeting their legal and regulatory obligations.

Defend

As one of the few organisations in our sector to have achieved ISO 27001 information security certification, we will build the requirements of the GDPR into our existing framework to protect the security and integrity of all of the data we process.

Prevent

We will continue to develop and strengthen our controls to identify vulnerabilities so that we can anticipate potential incidents before they occur.

Respond

Our Group will be transparent in the way in which we communicate to our customers so that we can continue to protect the rights of our data subjects.

FOREWORD

Donald Fowler,
Chief Executive, Premex Group.

The recent global ransomware attack has highlighted that adequate and effective information security is paramount to any business.

We, the Premex Group of companies, have always recognised the importance of information security and the need to manage this as a fundamental aspect of our internal risk and governance framework.

In 2014 our commitment to this cause propelled us on a journey that not only resulted in certification under the globally recognised ISO/IEC 27001:2013 standard, but it also brought about a cultural transformation across our businesses in the UK.

Our overall aim has always been, and will continue to be, the integration of information security as a core consideration in each and every process spanning the length and breadth of our UK Group. We have a dedicated team in place of compliance, legal and IT security professionals who provide support and guidance to our Group to ensure our staff recognise and prioritise the protection of data.

With the introduction of the General Data Protection Regulation coming in May 2018, we wanted to take this opportunity to assure our customers of our ongoing commitment to information security and the steps we are taking to strengthen our governance controls, so that we can continue to meet and exceed our legal and customer requirements.

We hope you find this overview helpful and invite you to contact our GDPR project team with any questions you may have, or to request further information about how we are working towards GDPR compliance.

CONTENTS

WHAT IS THE GDPR?

25 MAY 2018

The EU General Data Protection Regulation (GDPR) is due to come into full effect from 25th May 2018, replacing elements of the current Data Protection Act 1998.

This regulation will create new legal obligations which will have a significant impact upon the way in which organisations must handle personal data.

WHO DOES IT APPLY TO?

It applies to all organisations - public and private, anywhere in the world that **handle, store or process the personal data of EU citizens.** GDPR dictates the procedures and consequences surrounding data breaches and notification requirements.

THE CONSEQUENCES OF NON-COMPLIANCE ARE SEVERE:

FINES OF UP TO £20m

OR 4% OF GLOBAL TURNOVER

The risk of class action lawsuits from data breach victims

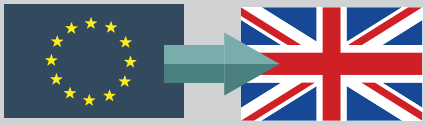
GDPR breaches must be reported within 72 hours

ORGANISATIONS MAY NEED TO APPOINT A DATA PROTECTION OFFICER.

Staff Training

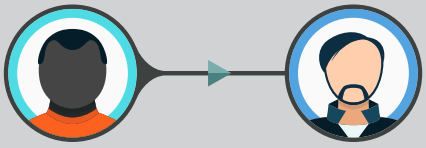
Internal Audits

Notifying the supervisor if there is a breach



The UK government has confirmed that our decision to **leave the EU** will not affect the introduction of the **GDPR**

GDPR will impact on both controllers and processors



All data being stored should be obtained by consent:

OPT IN

NOT OPT OUT

New rights for individuals such as the right to be forgotten and the right to data portability

Data subjects will have a **right of compensation** in respect of breaches

OUR GROUP'S APPROACH TO INFORMATION SECURITY

2014: Commenced project to achieve ISO/IEC 27001:2013 certification

2014

In **2014** our Group chose to pursue the internationally recognised ISO/IEC 27001:2013 certification to demonstrate our commitment to information security and continue to set the standard in our industry.

2016: We achieve ISO/IEC 27001:2013 certification

2016

In **2016** we achieved the highest standard of information security across our sites at Bolton and Durham, providing customers with complete assurance of our commitment to protect all data.

In order to meet the requirements of the **GDPR** we are now building upon our existing information security management system (ISMS)

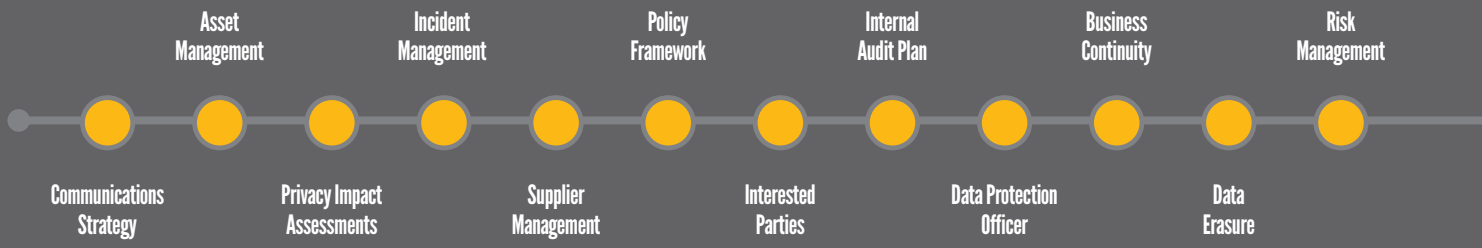
2017

2017: Build GDPR '**Prevent & Respond**' framework

2018

2018: The **GDPR** comes into force

OUR GROUP'S GDPR PROGRAM OF WORK



ENSURING GDPR COMPLIANCE

POLICY FRAMEWORK

Our policy framework forms a fundamental part of our information security management system as it sets out the principles we apply as a Group to protect information. Our Group will review existing principles and policies to ensure they are in line with the regulation's requirements.

FAIR PROCESSING NOTICE

Our Group understands the importance of transparency in data processing. Our fair processing notices will provide clear guidance to data subjects on how our Group will handle and process information as well as be a point of contact for any questions.

CONSENT

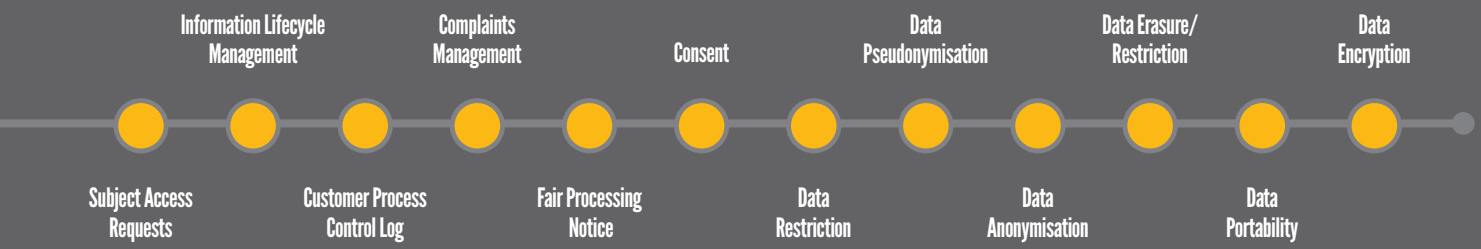
Our Group has always sought consent to process personal data and provides clear guidelines to data subjects on how we will process and handle their data. We will seek to ensure existing controls around consent meet the requirements of the GDPR so that we are truly transparent in our processes.

PRIVACY IMPACT ASSESSMENTS

Our Group has always embodied the philosophy of privacy by design and default. With a dedicated change management function in place across the Group we are able to consider privacy from the outset of any change. This way we can ensure we integrate the requirements of the GDPR throughout the lifecycle of a change.

SUPPLIER MANAGEMENT

We recognise that third party suppliers are an area of risk for the Group.
Our supplier management program is a fundamental aspect of our control framework. All suppliers are assessed and, where applicable, audited on the basis of risk and controls and contractual provisions are applied accordingly.



INCIDENT MANAGEMENT

Our Group is continuing to build upon existing processes to ensure any incidents are identified and managed swiftly and in line with the regulation.

SUBJECT ACCESS REQUESTS

Our Group has controls in place to respond to any requests from data subjects. As part of our program of work we will look to develop these controls so that we can meet the reduced timescales for the provision of data in line with the GDPR.

If you have any questions or would like to discuss this with us, please feel free to get in touch. Otherwise we would be grateful if you could return the attached signed copy of the Addendum to ensure that we both fulfil our obligations under GDPR.

CONTACT DETAILS:

We welcome any questions you may have in relation to our framework and invite you to contact either our Group Compliance Manager, Natasha Andrews, **natasha.andrews@premex.com** or our General Counsel and Head of Compliance, Caroline Russell, **caroline.russell@premex.com**.

premex group