

# THE IT MANAGER'S GUIDE TO GDPR



This infographic has been formulated to give 'Team IT' a guide on the milestones and key tasks required to achieve GDPR compliance. By following this journey you'll have the foundations of a strategy to your organisation ready for the big switch on in May 2018.

## 2016

NOV

Attend Foursys Webinar: IT Manager's guide to GDPR - getting your department up to speed and ready...

(Or watch on our YouTube channel if you missed it!)



YouTube

Understand the legal grounds on which you collect and use data, *specifically consent!*

REVIEW IT SYSTEMS AND PROCEDURES.

? Can your organisation technically cope with new individual rights in a timely manner?

? Can you perform right to be forgotten, recording objections, deletion of information and subject access requests.

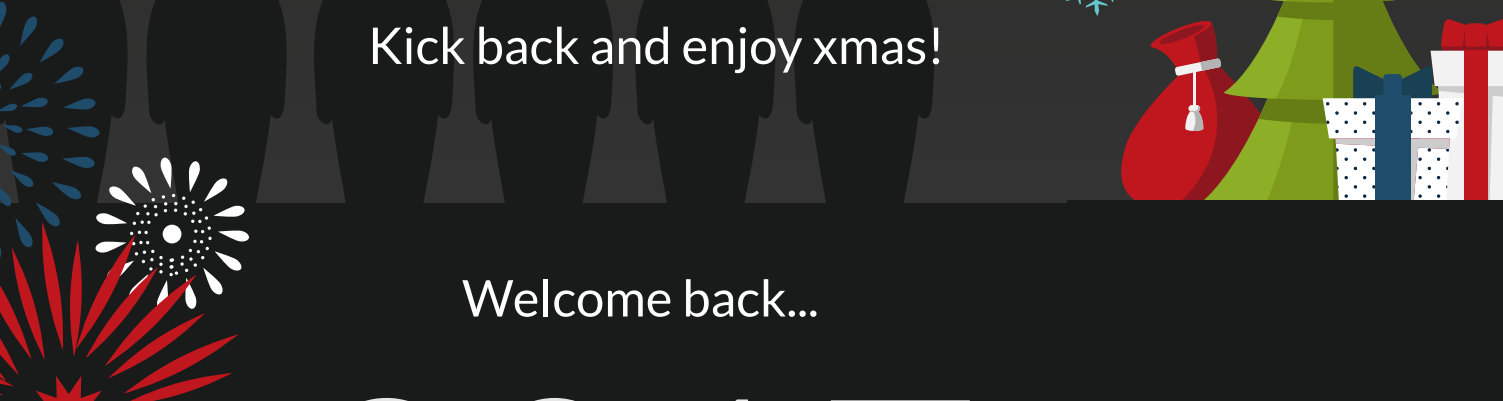
REVIEW CURRENT DATA SHARING PROCESSES AS IT APPLIES TO GDPR REGULATED INFORMATION.

? Does your organisation understand data flows in and out of the organisation?

? Can they identify which information has been shared and with who? Right to be forgotten extends to partners. And you may also be asked to 'forget' information as well.

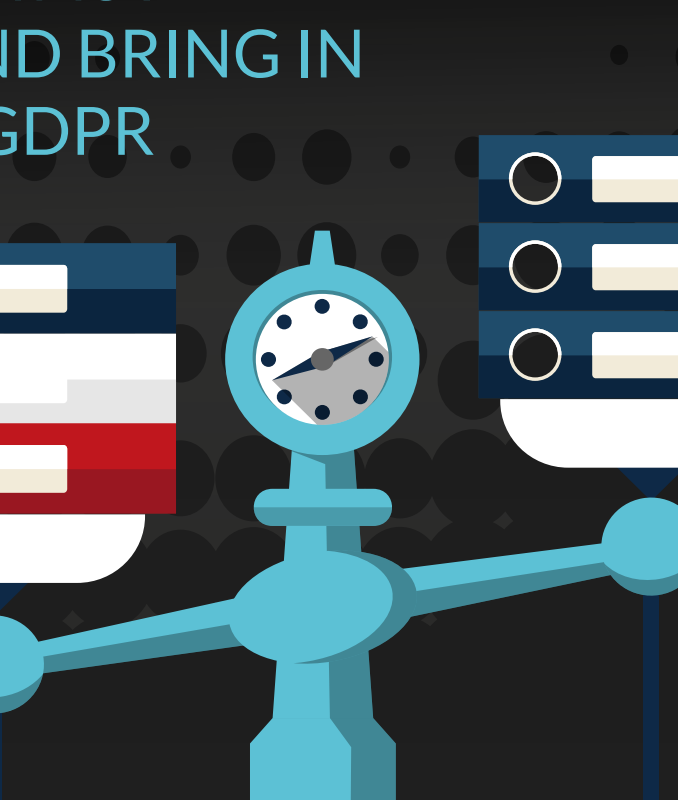
REVIEW STAFFING REQUIREMENTS, DESIGNATE A DATA PROTECTION OFFICER (DPO) OR AT THE VERY LEAST SOMEONE RESPONSIBLE FOR GDPR COMPLIANCE AND BUILD A SUPPORTING TEAM.

Note that this lead position can be outsourced to a competent firm or individual, which is an option that smaller organisations may wish to consider.

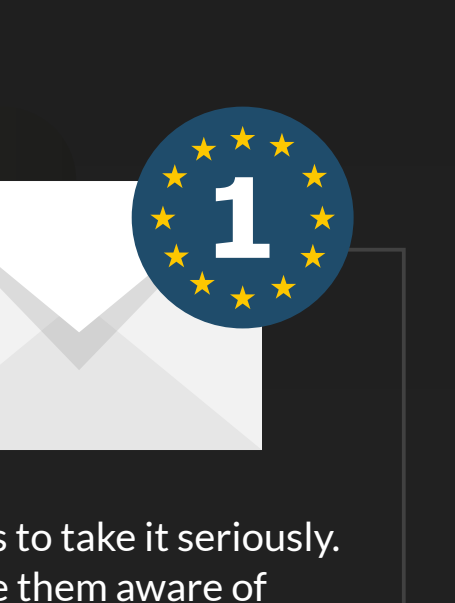


Build an outline plan for compliance, including rough budget contingency for any new personnel, consulting resource and technology. This might be the last chance to get budget approval and have time to implement before the regulation comes into play.

## SUBMIT YOUR GDPR CHANGE PROPOSAL TO MANAGEMENT



Kick back and enjoy xmas!



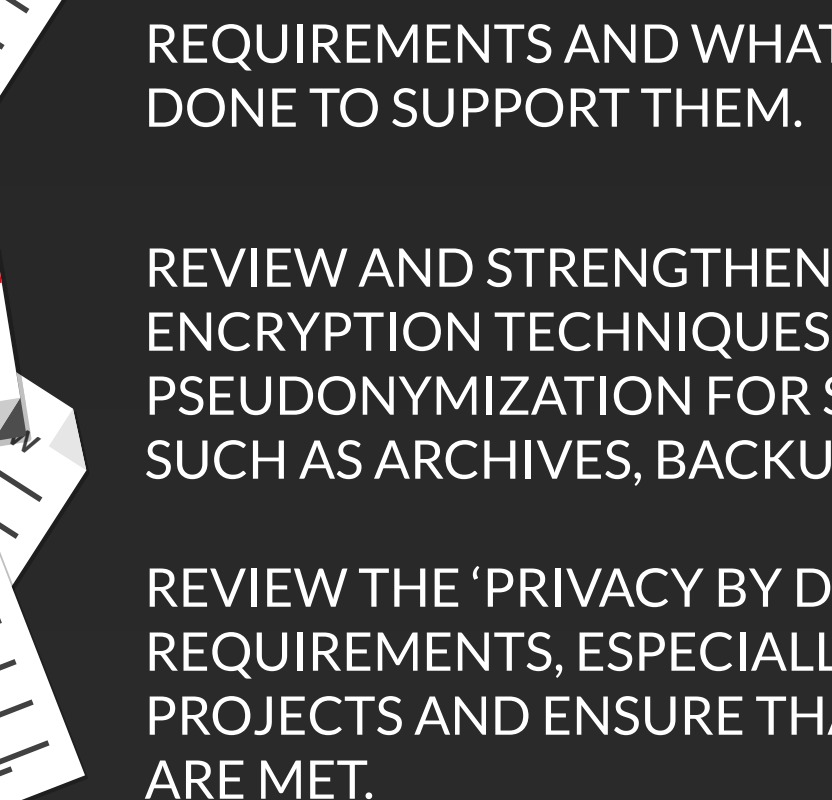
Welcome back...

## 2017

BEGIN DATA DISCOVERY EXERCISE WITH THE USE OF FOURSYS FREE ONSITE GDPR DATA ASSESSMENT.

Ensure your DPO has access to reports/metrics from the technical controls deployed throughout the timeline. This will enforce the tuning requirement of the GDPR for both technical and organisation controls.

JAN



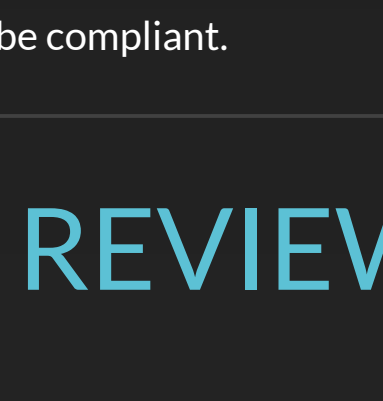
REVIEW PRIVACY NOTICES AND BRING IN LINE WITH GDPR



FEB

BEGIN STAFF COMMUNICATIONS AROUND GDPR

What it is, when it comes into force and why the business needs to take it seriously. There could be a regular monthly newsletter to all staff to make them aware of specific pieces of GDPR and what you will need to do to be compliant.



## ASSESSMENTS AND REVIEWS

MAR

REVIEW FOURSYS GDPR DATA DISCOVERY REPORT AND BEGIN TO COMPILE DOCUMENT AND TECHNOLOGY REQUESTS FOR ANY CHANGES REQUIRED. PRIORITISING AREAS WITH HIGHEST RISK AND MOST IMPACT.

APR

CONDUCT DATA PROTECTION IMPACT ASSESSMENTS (DPIA) / PRIVACY IMPACT ASSESSMENTS FOR RISKIER ACTIVITIES.

MAY

EXAMINE THE DATA PORTABILITY REQUIREMENTS AND WHAT NEEDS TO BE DONE TO SUPPORT THEM.

JUN

REVIEW AND STRENGTHEN THE USE OF ENCRYPTION TECHNIQUES OR CONSIDER PSEUDONYMIZATION FOR SOME DATASETS SUCH AS ARCHIVES, BACKUPS.

JUL

REVIEW THE 'PRIVACY BY DESIGN' REQUIREMENTS, ESPECIALLY FOR NEW PROJECTS AND ENSURE THAT THE NEEDS ARE MET.

NOV

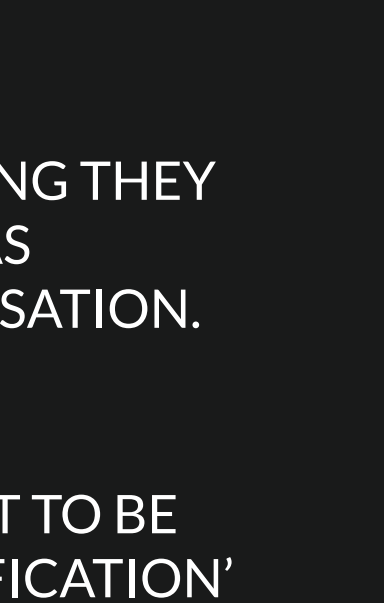
SET UP PROCEDURES AND POLICIES FOR DATA BREACH IDENTIFICATION AND ESTABLISH THE PROCESS FOR NOTIFYING THE INFORMATION COMMISSIONER'S OFFICE (ICO) AND AFFECTED INDIVIDUALS.

IMPLEMENT REQUIRED CHANGES DISCOVERED IN PREVIOUS MONTHS AND SCHEDULE IN TRAINING SESSIONS FOR ALL STAFF ABOUT GDPR COMPLIANCE AND CHANGES MADE WITHIN THE ORGANISATION.

REVIEW AND AUDIT COMMISSIONING SUPPLY CHAIN AND UPDATE CONTRACTS.

GIVE SPECIFIC FOCUS TO CONTRACTS WITH ANY CLOUD PROVIDERS AND THE ADEQUACY OF MECHANISMS FOR CROSS-BORDER TRANSFERS WITH THEM.

Buy your DPO a present its that time again!



This is the year!

## 2018

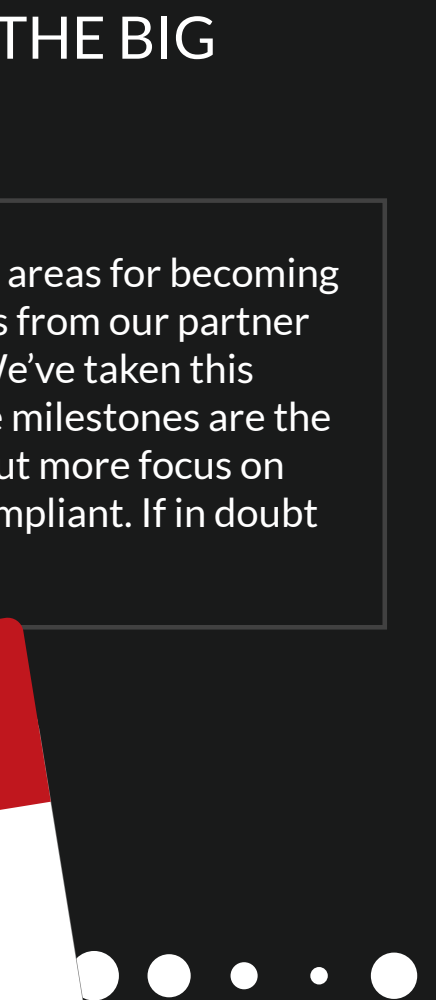
JAN

REVIEW CHANGES MADE, ENSURING THEY ARE EMBEDDED AND WORKING AS DESIGNED WITHIN YOUR ORGANISATION.

FEB

RUN SOME SCENARIOS, E.G. 'RIGHT TO BE FORGOTTEN' AND 'BREACH NOTIFICATION' TO ENSURE THAT THE PROCESSES ARE OPERATING EFFECTIVELY.

Ensure that your DPO (Data Protection Officer) is happy with everything that's in place – There is still time to make changes if required!



APR

YOUR ORGANISATION IS GDPR COMPLIANT, YOU'VE RAN THE LAST COMPLIANCE AND TECHNOLOGY CHECKS AND YOUR GDPR COMPLIANCE OFFICER IS SATISFIED YOU'RE READY FOR THE BIG SWITCH ON NEXT MONTH!

This timeline has been produced off the basis of the 12 ICO focus areas for becoming EU GDPR compliant and through the guidance of GDPR experts from our partner organisations as well as our own knowledge and research. We've taken this information and tailored it specifically for the IT team. The above milestones are the foundations to checking you have the fundamentals in place but more focus on specific areas may be required to get your organisation GDPR compliant. If in doubt consult your DPO or contact Foursys.

