Winckworth Sherwood

Where to start

A. Raise awareness within your organisation of the need to comply including obtaining board level buy-in and budget and train relevant staff

B. Assemble a cross-functional GDPR Response Team including Legal, Compliance, IT and your Data Protection Officer

How to ensure your compliance programme is on track

1. Stop collecting data you don't need
2. Stop using it for something other than what it was collected for
3. Be transparent
4. Be accountable

What to do after May 2018

GDPR: 5 Step Action Plan

What to do now

If audit reveals security risks, accelerate your security review

1. Map your data

Questions to ask:

1. Where is my data?
2. Where does my data come from?
3. Why are we collecting it?
4. Where is data held?
5. Where does it go around the company?
6. Who has access to the data? What are their skills, clearance & training?
7. How sensitive is the data (personal, sensitive, anonymous)?
8. What 3rd parties is it shared with? How is it transferred?
9. What agreements and contracts do you have with processors?
10. How is data transferred overseas?
11. Where are your Cloud servers?
12. What encryption is used?
13. Does your data leave the EEA? If so who 'exports' it and who receives it?

a) If your data leaves the EU what method is used now (e.g. model clauses)?

b) Would binding corporate rules work for your organisation?

3. Contract Review

Consider & review:

1. Supplier contracts from data processors
2. Contracts where you are the processor
3. Joint data controller contracts
4. Prioritise contracts according to risk (not value, necessarily)
5. Upgrade IT to add functionality

(i) Keep a log of all consents (e.g. web, social media, digital, contract)

(ii) Offer a 'right to be forgotten'

(iii) Allow objections to profiling

(iv) Allow 'data portability'

6. Also consider:

A. "Privacy By Design" built into each system change

B. "Data Protection Impact Assessments" for major system overhauls

4. Review Data Security

1. Are there adequate firewalls and virus protections?
2. Is there a clear password policy? Is it enforced?
3. Is there a procedure in place for data breach management?
4. Who is responsible for it?
5. Do all staff understand the procedure?
6. Include response, notification process recovery and damage limitation
7. Include risk assessment for the consequences of the breach?
8. What investigative process is triggered to ascertain the cause of the breach and if response can be improved?
9. Test breach management procedure with a 'mock' breach
10. What do you do with your data when you aren't using it?
11. Review storage and data elimination/destruction policies

5. Implement New Processes

Update and implement new processes:

1. New consent formats and refresh old consents
2. Stop relying on consent where you should not do so (e.g. employees)
3. New fair processing notices (both for customers and employees)
4. New privacy policies
5. New data retention policy
6. New DSAR process & training
7. Processes to implement new rights (e.g. erasure, correction, portability)
8. New breach reporting process
9. New model clause contracts (if needed)
10. Refresh staff training

12 Step 24HR Data Breach Response Plan

1. Mobilise crisis management team with support from communications and legal advisers, as appropriate

2. Record the date and time when the breach was discovered, as well as the current date and time when response efforts began, i.e. when someone on the response team is alerted to the breach

3. Alert and activate everyone on the response team, including external resources, to begin executing your incident response plan

4. Protect your reputation with an internal and external communications strategy, supported as necessary by crisis communications specialists and/or reputation lawyers

5. Secure the IT systems affected by the cyber attack to help preserve evidence

6. Stop additional data loss. Take affected equipment offline but do not turn them off or start probing into the computer until your forensics team arrives

7. Document everything known thus far about the attack

8. Interview those involved in discovering the breach and anyone else who may know about it

9. Review protocols regarding disseminating information about the breach for everyone involved in this early stage

10. Bring in your forensics team to begin an in-depth investigation

11. Report to police, if/when considered appropriate

12. Notify regulators, if needed, after consulting with legal counsel and upper management and insurance broker(s) to ensure compliance with policy terms

DISCOVERY | UPDATE | PREVENTION | IMPLEMENT | CHECKLIST | BEYOND

Not ok

Silence
Pre-ticked (opt-out)
Inactivity

OK

12

Verify age
Verify parent or guardian consent

OK

Tick box (opt-in)
Wet signature
Affirmative action

2. Update consents & privacy policies

Consider & review:

1. What consents do you have and are they GDPR compliant?
2. Customer journeys and terms and conditions
3. Marketing, competitions and promotions
4. Fair processing notices
5. Privacy Policies
6. Website terms
7. Who is your current DPO and can they be your GDPR DPO if you need one?

See overleaf for how Winckworth Sherwood can help your organisation to become GDPR compliant

TONI VITALE
HEAD OF REGULATION, DATA & INFORMATION
020 3735 1934
tvitale@wslaw.co.uk
wslaw.co.uk/GDPR

Winckworth Sherwood

CHECKLIST

1. Raise awareness within organisation
2. Form GDPR team
3. Complete data audit & gap analysis
4. Update/refresh consents
5. Update contracts
6. Update policies
7. Appoint a DPO
8. Roll out new customer terms
9. Review security
10. Train staff

FOLLOW-UP

Consider & review:

1. What consents do you have and are they GDPR compliant?
2. Customer journeys and terms and conditions
3. Marketing, competitions and promotions
4. Fair processing notices
5. Privacy Policies
6. Website terms
7. Who is your current DPO and can they be your GDPR DPO if you need one?
8. Audit suppliers and supplier contracts

Existing customers
Can you prove you have clear explicit permission for all uses of the data you hold?
Have you informed them of their rights to:
1. Object to profiling?
2. Erase data?
3. Transfer their data to someone new?
If the answer is No to any of these questions you may need to 'refresh' your consents

New customers
Start sending the new data protection policy setting out the new rights and a new fair processing notice
Data protection safeguards must be built into products and services from the earliest stage of development
(Privacy by Design) (See also step 3 if additional IT functionality required)

Annual contracts
Start sending customers new data protection policies which set out their new rights and a new fair processing notice

How can Winckworth Sherwood's GDPR team assist you?

1	Raise awareness	Helping you prepare and deliver: Board presentations Training FAQs
2	Data audits	Data Audits Surveys Mapping *Please ask for our sample audit questionnaires*
3	Update privacy processes/DPO appointment	Reviewing & updating: Fair processing notices Website terms Privacy policies DPO Appointments: *Please ask for our guide to DPOs including a job specification*
4	Customer & consent review	Reviewing consents & whether they should be refreshed Code of contract for suppliers
5	Contract review	Supplier/third party contract review New contract terms Amending existing contracts Negotiation training for procurement teams
6	Map overseas data transfers	Review international data transfers Consider Binding Corporate Rules Review use of model clauses
7	HR processes	Review HR & internal policies and procedures, including fair processing notices, privacy policies and contracts – avoiding reliance on consent
8	DSAR & breach reporting	Review subject access request processes DSAR training Review how other rights will be implemented Review breach reporting processes
9	Security review	Review & update security processes & policies Guidance on what to do in the first 24 hours after a breach Training on how to avoid reputation issues post breach Review
10	DPIA support	Conducting Data Protection Impact Assessments Assessing whether a DPIA is necessary *Please ask for our DPIA assessment checklists*

Helplines: We offer the following data protection helpline services (rates are fixed, and unlike a retainer you only pay for the time you use):

- **GDPR General Helpline** – To deal with adhoc queries and questions.
- **GDPR Emergency Data Breach Helpline** – Assisting in the immediate aftermath of a data breach, advice on whether the breach is reportable and the steps you should take in the first hours/days after a breach (includes out of hours support for evenings and weekends).
- **ICO Investigations Helpline** – Advising you as to how to handle an ICO investigation and how to mitigate the potential sanctions against you.

Contact **Toni Vitale** at tvitale@wslaw.co.uk for more information.

wslaw.co.uk/GDPR

Winckworth Sherwood