GDPR for SME and clubs

A Tranlowe Perspective

Revised: November 2017

Written by Craig Tranfield of Tranlowe Ltd,

Craig.Tranfield@tranlowe.co.uk

www.tranlowe.co.uk

1. Contents

Table of Contents

Introduction

With the General Data Protection Regulation (GDPR) coming into force on 25 May 2018 there are a vast array of commentators, who all seem to say much the same "nothing useful" and merely reflect a management responsibility without any practical suggestions on what anybody needs to actually DO. Apart from stating the obvious, which they often do, they lack implementation guidance.

Conversely, the starting point for this perspective is to see what the regulation actually says to see who is affected or excluded, and what it means for them, particularly if they are not a big business.

The basic question of "Who?" is readily addressed by looking at Recital 18 of the regulation supported by Article 2.2c:

> (18) This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.
>
> Article 2.2.This Regulation does not apply to the processing of personal data: …
> (c) by a natural person in the course of a purely personal or household activity;

So domestic use is exempt, BUT EVERYTHING ELSE must comply!

This paper is therefore written with the intention of supporting not just SMEs but also micro-enterprises and clubs where technical resources and manpower are more limited. If you are either a larger business or handle large amounts of data then this paper is insufficient for your needs.

At 88 pages the regulation is too long to reproduce here but particularly relevant extracts are in Appendix 1 so you can cross reference why I make the proposals that I do, and look up the full text.

I will start with **what is needed as a single page!** The rest is appendices initially listing the extracts just mentioned and then samples of what it means in practice. The final section is a correlation of what I have written here with the summary produced by the ICO[1] as a 12 Step plan[2], although you may also wish to read their guide to small businesses (updated 21-nov-17) at: https://ico.org.uk/for-organisations/business/.

You are welcome to use this paper to generate the necessary policies and records for GDPR compliance yourself but if you might be interested in some support then please contact me at Craig.Tranfield@Tranlowe.co.uk

1 ICO is the Information Commissioner's Office, https://ico.org.uk/
2 https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

Tranlowe is a small independent business based in Woodford, London and Truro providing Information Security and Computing Infrastructure review and assessment services.

Craig Tranfield has worked in the IT industry for over 30 years although he initially trained in building technology/civil engineering (BSc). At first he left the building sites to work in computer 3D modelling of buildings and services. Moving from software development to systems and operations management (MSc, MBCS, CEng, CITP) Craig became more engrossed in the management side (DipMgt). Whilst continuing with computer management, predominantly at Oxford University Department of Computer Science Craig kept his hand in on computer networks (CCNA) and then focussed on Information Security (CISSP).

What do you need

Starting from before you get the data, you need to decide just what you need and why. This means that you must **write a Privacy Statement** (see Appendix 2.1) to present to the data subjects so that when you request the data they can give informed clear **consent** (see Appendix 2.2), which you will then **record for future reference.** This needs to state how you will use it, and for no other uses. [R32, 39, 40, 42/Article 4.11, 5.1a, 6, 13.1-4]

Having got some data, you need to have a policy and supporting processes to **ensure that the data is current**, either by the way it is updated or as part of the retention constraints. [R59, 63 /A4.11, 5.1a, 6, 13.1-4] This requires having a **Process description** of how subjects **request changes**, including deletion (see Appendix 2.3).

Indeed, there are a whole swathe of details you need to hold about the data, in what we might call an **Information Asset Register,** which could simply be a spreadsheet! (See Appendix 2.7).

And all that is before you even use the data! When you do so, you need a **description** of the **process you will run** (see Appendix 2.4), and to maintain a log of the usage. [R82] However, this is not limited to what you do first hand as whilst you remain responsible for the data, you can use foreign services so long as they are either subject to rules in the listed permitted countries or other suitable conditions. [R22/A45 (see links in notes to A45)]

However, recognition is given both to the correlation between organisational size and capacity for administration [R13/A30 say that the degree of record keeping is less for smaller organisations] and importance for that administration in relation to the sensitivity of the data you handle [R84/A37.1].

The final area to be addressed, and a significant motivator to many for going through all this in the first place, is what to do when it goes wrong. This could be as simple as sending an email with confidential details to the wrong address, accidentally deleting/ disk crash losing important data, or the more publicised events such as being subject to ransomware or a hacker stealing a copy of the data you hold, or for what ever reason, initiated by a data subject lodging a complaint [R141/A77, 79, 82.1, 83.5]. Mitigation is expected both as pre-emptive measures and reactively as an **Incident Response Plan** (see Appendix 2.5). Within that, there needs to be the instructions on how to **notify the authorities** and individuals affected (see Appendix 2.6). [R85, 86]

That is the lot. Know what you have got, why you have it, what you do with it, and where you have it, then you can take reasonable care of it, and know when you have finished with it so you can get rid of it. Record that lot and you will be in a far more defensible position when challenged or something goes wrong.

Appendix

1 The Regulation, extracts

The Regulation comprises 2 parts, the first is called “Recitals” of which there are 173 laying out the context and objectives, and secondly there are 99 “Articles” which state the rules.

The contents of this appendix are presented as:

> (Recital number) extract of text.
>
> *My interpretation and paraphrase with reference to associated Articles and other useful cross references.*

1.1. Recitals referenced

(13) ...To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping.

Aka: There is a sense of proportionality, larger organisations having greater capacities than smaller ones.

(22) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union...

Aka: you can’t send the problem abroad, and use of cloud services need to comply, Article 3.1, 44, and only send abroad if that country is approved, Article 45. The Safe Harbor agreement is no longer valid for USA but replaced by “Privacy Shield” where businesses have been certified by US Dept of Commerce, see links in notes to A45.

(26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.

Aka: simple cross references don’t stop the data being personal, Article 4.5, although see 28 below.

(28) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations

Aka: ...it does make it safer.

(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.

Aka: no trying to get it on the quiet, must be informed and explicit, so you have to lay out to what you are asking them to agree. Article 4.11, 13.1-4, see also Recital 42.

(38) Children merit specific protection with regard to their personal data...

Aka: children can't give consent, this has to come from the guardian until they come of age, but that also defers the start of the data retention period. Article 8.1 states that a child is up to age 16. However, the UK Data Protection Bill 2017, section 8a, proposes reducing this to 13 as an age for consent.

(39) Any processing of personal data should be lawful and fair...the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed...Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing

Aka: you have to lay out why you need what, not ask for more than the minimum necessary, and delete it as soon as practical after finished with it whilst ensuring that it is accurate and not out of date. Article 5.1a & Article 6.

Furthermore, you have to take suitable care of the data. Article 32.1.

(40) In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law...

Aka: unless there is a legal obligation (eg. UKBA, HMRC, (44) inter-party contracts...) you need to have got consent.

(42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation.

Aka: Don't lose the record of consent being given! Article 5.2, 7.1

(51) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection

Aka: some data is not just personal but also sensitive. Article 9 defines this as "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, ...genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation..."

(59) Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object...The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

Aka: you have to give people chance to see if you have data on them and if so what, Article 15, get it corrected, Article 16, retract consent Article 7.3 & 18, and get you to delete it, Article 17, and to do so "within 1 month", Article 12.3 with exclusions in 12.5. See also recital 65 for a 'right to be forgotten', Article 17.

(63) ...Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data....

Aka: if the user maintains the data then recital 59 is significantly solved.

(65) A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten'...

Aka: as per 59 above.

(76) ... it is established whether data processing operations involve a risk or a high risk.

Aka: In Risk Analysis indicate alternative levels.

(82) In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility...

Aka: Document all processes utilising personal data, see comment on Article 30 below.

(83) ...In assessing data security risk, ... such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

Aka: The "CIA" model, Confidentiality, Integrity, Availability.

(84) ...where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk.

Aka: even if small, need to handle more sensitive data more carefully.

(85) A personal data breach may, if not addressed in an appropriate and timely manner...the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons...

Aka: You need to know how to respond "in an appropriate and timely manner" at the start of an incident to minimise the impact, Article 33.3d, and (where relevant) you don't have long to report it! Article 33. Further, Article 33.5, you need to record it.

(86) The controller should communicate to the data subject a personal data breach,...

Aka: you also have to tell the people.

(141) Every data subject should have the right to lodge a complaint with a single supervisory authority...

Aka: anyone affected can notify the authorities.

1.2. Articles referenced

(3.1) This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

(4.5) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information...

(4.11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(5.1) Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')...

(5.2) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

(6.1) Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes...

(7.1) Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

(7.3) The data subject shall have the right to withdraw his or her consent at any time...

(8.1) ...Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

(9.1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Although 9.2-4 lists the exceptions.

(10) Processing of personal data relating to criminal convictions and offences or related security measures...

(12.3) The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by...

(12.5) Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive...

(13.1) Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information...

(15) The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:...

(16) The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her....

(17) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay...

(18.1) The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:...

(30) If organisation has more than 250 people employed, *or 30.5* "...the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10." then need to keep a record of what processing happens, purpose & dataset, to whom disclosed, when due for deletion, and security used, 30.1-4.

Aka, most clubs and SME will be relieved of this level of record keeping but check the wording against what you are handling.

(32.1) "...ensure a level of security appropriate to the risk, including inter alia as appropriate:"

Aka, you aren't expected to do everything but nor can you get away with doing nothing, be proportionate in your controls.

(33.3d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

(33.5) "The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken..."

(35) where processing “likely to result in a high risk to the rights and freedoms of natural persons...” assess impact on security of the data and if need mitigation notify authorities, Article 36.

Aka, even if you are small, cf Article 30, if you are working with highly sensitive data then you need to go further than this paper addresses.

(36) The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

Aka, there can be circumstances where your business needs to get approval for what it does.

(37.1) Need a Data Protection Officer (DPO) if handling large scale data or a public authority

Aka, the target audience of this paper would not require a DPO, but as with Article 35 above, if you do, then this paper by itself is insufficient for you.

(44) Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if...

There are then 9 qualifications.

(45) A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection.

Aka, Transferring data outside EU, such as using cloud facilities hosted abroad, is acceptable to approved countries, see
http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm,
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/, and
https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/, and additionally to businesses in other countries where there is a specifically certified list of approved businesses such as those registered with Privacy Shield in the USA,
https://www.privacyshield.gov/article?id=How-to-Verify-an-Organization-s-Privacy-Shield-Commitments, or
where the transfer is covered by suitable contractual agreements.

Check where you send data!

(77) “...every data subject shall have the right to lodge a complaint with a supervisory authority...”,
(79) “each data subject shall have the right to an effective judicial remedy”,
(82.1) “...shall have the right to receive compensation from the controller or processor for the damage suffered...”.
(83.5) “...fines up to 20 000 000 EUR...”

Aka: misuse data and you are liable for legal action which could lead to payment of significant compensation!

2 Sample Texts

2.1. Privacy Notice

The following sample is aimed at organisations who only hold membership/supporter details acquired via written paper forms and/or email. Where there is a website it should just give out information, and have contact via email, and hence no data acquired through it. Even tickets, for example, may be sold through a 3rd party who handle payment details and purchase contact details rather than yourself.

This sample needs significant customisation and the end product is likely to run to 4 pages, so this is not a noddy piece of text. You may choose to tier the information provided so as not to confront your users/data subjects with a mass of text in one go. You will therefore have to think about how you will make it available to them.

Since this is in effect a contract the necessary information is to identify the parties (who you are), identify why you want what off them, what you will do in return and the limits of that, and how they can indicate their agreement.

For example, consider a club, it would need contact details for members, some record of relevant abilities (instrument if an orchestra), subscription and other payments, contribution to activities of the club (matches played in or administrative posts held), external affiliations (avoid conflicts of interests) or rankings (pick best players for teams), age or health issues (to offer concessions), emergency contact details.

Privacy Policy template text

<Name of organisation> ("**we**", "**us**" or "**our**") is committed to protecting and respecting your privacy. [We own and operate the <website URL>]

In this Privacy Policy, references to "**you**" are to any person who submits data to us [or the Website] about him/herself or about any living individual.

This Privacy Policy (together with any other of our terms and conditions, and any other documents referred to in them) sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us. Please read this Privacy Policy carefully to understand our views and practices regarding your personal data and how we will treat it.

We will only use your personal data in the manner set out in this Privacy Policy. We will only use your personal data in a way that is fair to you based on your consent. We will only collect personal data where it is necessary for us to do so and where it is relevant to our dealings with you. We will only keep your personal data for as long as it is relevant to the purpose for which it was collected or for as long as we are required to keep it by law.

Your name and (email) address, or telephone number will be used to inform you regarding [upcoming events, delivery of tickets...] and changes in this Privacy Policy Statement. These details may be passed to other members to facilitate such membership.

Other than as set out in this Privacy Policy, we shall NOT sell or disclose your personal data to third parties without obtaining your prior consent unless this is necessary for the purposes set out in this Privacy Policy or unless we are required to do so by law.

We will record payments made, evidence may be required where concessional rates are sought. This information will be passed to auditors, or similar, as legally required.

Normal operation of <club> activities further requires recording of data such as participation in <the club>, <scores, ranking, awards...>

You should only submit to us <or the Website> information which is accurate and not misleading. You should keep that information up-to-date and let us know as soon as possible of any changes to that information by <email/ written note to secretary...> at <club contact address>.

By submitting your or anyone else's data to us <or the Website>, you must ensure that you have full authority and consent to supply us with that data on their behalf and you warrant to us that you have that authority.

You are advised that you have the right to have your data amended to remove errors, to withdraw your consent for some or all processing, and to have you records deleted. For these purposes you may contact <us | the controller><means and details/phone, address, email...>. Possible consequences of such changes to consent will be loss of benefits provided by processes from which you opted out. You further have the right to lodge a complaint with the supervisory authority, <ICO>

Any correspondence may be recorded.

This Privacy Policy was most recently updated on < date of review>

A small business may also include text similar to:

We may transfer our databases containing your personal information if we sell our business or part of it to an actual or potential purchaser.

We may share your data with third parties that work with us at Events, for example sponsors and exhibitors at Events we deliver and that you attend. If you book to attend an Event, you consent to us sharing your data with such third parties, and to those third parties contacting you with marketing communications following the Event about the products and services they provide. If you do not want us to use your data in this way, or to pass your details on to third parties for marketing purposes, please contact us at <business contact> and we will update your privacy.

By attending an Event, you consent to be photographed, filmed and/or otherwise recorded in a group setting at the Event. Where your badge/personal details are legible, we will contact you to seek your permission prior to publication.

Please note that you can revoke any consent you have given us under this policy at any time by contacting us at <contact>.

Any changes we may make to this Privacy Policy in the future will be [posted on the Website and, where appropriate,] notified to you by <e-mail or letter>. [Each time you enter the Website, you agree that the Privacy Policy current at that time shall apply to all information held by you.]

2.2. Consent statement

Where a paper form is used, after you have provided the space for the user to insert their data you may write:

By signing this form you consent to our use of the data provided in the ways specified in the Privacy Policy.

Signed:..... Date:.....

You may also put tick boxes against items such as phone number or address for them to indicate their consent for specific purposes, for example, newsletter distribution or membership directories.

If there is a web form then there could be:

Please tick this box before submitting this form to indicate your consent to our use of the data provided in the ways specified in this Privacy Policy.

[and then a tick box and a Submit button. Within the form processing note IP address, other data to evidence who has completed the details, add a time stamp, and record it]

2.3. Description of Processes Initiated by Data Subjects

Data Change Request

This is to describe both what the data subject has to do to register a change request to either their personal details or their privacy authorisation, and what you need to do to validate and effect that change. This expands upon the Privacy Policy statement "You should keep that information up-to-date and let us know as soon as possible of any changes to that information by <email/ written note to secretary...> at <club contact address>."

The data Subjects

- Data Subject writes a note stating change to be made and signs it.
- Hands note to secretary, or posts it

or

- Data Subject writes an email stating change to be made

Internal processes

- Recipient authenticates request (personal recognition, seeks confirmation of request)
- Amends records, including deletion, see Article 17.
- Files change request

Other processes would include request for access to their data.

2.4. Description of personal data utilising processes initiated by you

Impersonal broadcasts (Newsletters, event promotion etc)

- Database search to extract all records where privacy setting permits contact for intended distribution
- transmit impersonal communique to each person via contact details

Mass distributions containing personal data

- Database search to extract all records where privacy setting permits contact for intended distribution
- Merge personal data with template communication into pre-distribution form
- Cross check result only contains the intended data fields
- Cross check security of distribution method is compatible with sensitivity of contents
- Cross check (second person where practical) that distribution mechanism correctly correlates message with intended recipient
- Distribute messages

Subscription and payment recording

- Scan membership records to identify who is liable for a subscription
  or
  Receive request to purchase (tickets or other)
- Cross check personal records for concessions eligibility
- Generate financial record of who owes how much at date for what (subscription/tickets/...)

- Cross check payments received against financial record of monies owed
- If “reason” owed is “Subscription”; Update membership record as subscription received
  If “reason” owed is “(Ticket or other) purchase”; Update sales record as charge paid
- Update financial records as money owed received

And likewise for other processes.

2.5. Incident Response Plan

Security incident classification assists determining the severity and criticality of the event and ensures that it receives the appropriate level of attention in terms of work priority and reporting. You may choose to use a classification scheme like that below.

Incident Classification,					
Incident factors	Score	0	2	4	8
Classification of Information Asset involved		Unrestricted	Restricted	Sensitive	Confidential
Extent of disclosure or unauthorised access to IA		None identified, potential event	Single or few within the organisation	Widespread within Club	Public
Amount of IA affected		Single or few items	Few	Many	Whole set
Ability to recover the IA in a relevant time frame		Yes	Possibly	No	Not at all
Relevance of integrity loss		Insignificant	Minor	Moderate	Major or Critical
Risk Analysis Impact rating		Insignificant	Minor	Moderate	Major or Critical

The score for each factor is added together and then the classification of the incident determined as:

non-event <= 2 < Low <=-8 < Medium <= 15 < High

These details are to be recorded in the Incident Record Form and the summary Incident Log, (Samples not provided)

For those potential incidents classified as “non-event” no further action is required. All other classifications require the event to be reported to others within given time frames, although escalation/de-escalation may happen subsequently, and resources applied at increasing priority as per the “Classification/Response” schedule (Sample not provided)

The actual response (Sample not provided) will then depend upon the type of incident such as…

- Accident v Attack
- Bodily (person gaining unauthorised personal access)
- Paper/ Computer files
  - Loss
  - Loss with (assumed) disclosure
  - Disclosure without loss
- Disclosure through attack

It is similarly important how reports and inquiries of the incident are handled internally, for customers, and for if the media should get involved. Therefore a range of formal statements for use under different circumstances should be prepared since under the pressure of the situation there will not be time to think of what to say so have a range to pick from like:
If you have a website and some other services have gone down you might put up...

> "Due to an ongoing incident services and contacts normally available here have been temporarily suspended. We look forward to being fully back on-line shortly."

For use by reception or other staff for medium level incidents you might use…

> "I believe that there has been an issue with part of a system causing some inconvenience, for any further details you will need to speak to the manager."

For a malicious incident, when admitting that there has been an incident you need portray the situation as being under control with senior management taking a lead rather than be defensive:

> "I believe that there has been an attack which got through to part of the system causing some inconvenience. For any further details you will need to speak to the Administrator who is directing the containment, investigation, and corrective action."

2.6. Data Breach reporting process

All data handlers should be made aware of who to notify in the case of even a suspected incident. That person should either Classify the incident or notify someone else who is able so to do. Once the severity is recognised then a suitably authorised person can organise the Containment of the incident, the Investigation, Recovery, and Remediation. As per Article 33.5 they must record "...the facts relating to the personal data breach, its effects and the remedial action taken..." This will then determine if there is a requirement to notify the "supervisory authority[3]".

2.7. Information Asset Register (IAR)

You can't manage and protect the data you hold unless you know what you have and where you have it. You also need to know the legal, and other, constraints upon how long you are allowed to hold it, which in turn calls for knowing how you got it when. This applies not only to personal data but you would do well to equally control your corporate and Intellectual Property (IP) data.

The Register, as distinct from the data itself, might come in 3 parts:

- Basic data identification
- Retention Reasoning
- Risk Assessment

3 In the UK the "supervisory authority" is the Information Commissioner's Office, ICO

Asset Register table 1: Basic Data Types and Collections Identification	
Field	**Reason**
Asset Identity	Means of referring to Register entry
Description	What is the set of data
Data Source	Paper form, web form...from the individual; or purchased database; other contact means
How consent received, held, and any constraints on usage	Need to demonstrate consent was given and for what uses, R32, 42/ A5.2, 7.1
Date acquired/updated data	Need to ensure it is current, R59, 63/ A4.11, 5.1a, 6, 13.1-4
Data “Owner”	Person responsible for managing the data and its entry in this IAR
Business Sensitivity Classification	More sensitive data requires more secure management R84 /A32.1, 35
Purpose for holding data	Justification for having it, R39
Personal or business data	To whom answerable for protection and usage of data
Sensitive Personal data-protection	More sensitive data requires more secure management R84 /A32.1, 35
Date Asset record reviewed	Need to check that this type of data is still relevant to the business function.

Asset Register table 2: Retention Reasoning	
Field	**Reason**
Who/What sets the data retention constraints	HMRC, UKBA, other legal requirement including business contracts, internal manager...
Retention Reasoning for value	How the different constraints have been applied and balanced.
Retention period start event	Basis from which to measure the retention period like “End of Tax Year” or member leaving club
Retention period	Duration (may be zero where it is more appropriate to define a “Retention ‘end’ event” rather than ‘start’)
Date Reviewed Constraints	Laws, best practice, and circumstances keep changing so you need to check that you are keeping up to date.

Asset Register table 3: Risk Assessment	
Field	**Reason**
How data is stored	You need to know where data is, including paper
What are the threats to how you hold it	Determine required protection, not just from “hackers” stealing a copy but the range of threats to Confidentiality, Integrity, and Availability
How is data moved or transmitted	You need to know what you do
What are the threats to such transmission	Determine required protection
Consequences if threat occurred	What would be the knock on outcome
Current Probability	How likely or far fetched are the threats?
Current Impact	How much does it matter?
<Calculated Risk rating>	Combination of Probability and Impact
Current Mitigation	How you currently minimise the threats
Target Probability	Might it be possible to reduce probability?
Target Impact	Is it possible to have any control over this?
<Calculated Target Risk Rating>	Combination of Target Probability and Impact
Planned changes to move towards Target Risk Rating	What plan to do about shortfall between Current and Target risk ratings – probably a reference to an external document
Progress on making those changes	You have to be able to demonstrate taking due care of data
Date Risk Assessment Reviewed	Check that assessment is not obsolete

Correlation to the 12 Steps from the ICO

1 Awareness

Check that the boss knows they have to make the business compliant!

2 Information you hold

“You should document what personal data you hold, where it came from and who you share it with.”

See appendix 2.7 Information Asset Register.

3 Communicating privacy information

Review Privacy Notice giving overview of purposes to which you will put their data *with statements on:*

1. How you intend to use the data
2. Legal basis for so doing
3. Data retention period (see IAR)
4. The user’s right to complain

See appendix 2.1 Privacy Notice.

4 Individuals’ Rights

Create processes to address each of their rights *including*:

1. How to report what data you have on someone, (see also step 5 below) both for their scrutiny and in a machine readable form for transfer to alternative processor
2. Process for them (once authenticated!) to have data errors corrected
3. Process for deletion of data (without your related records falling over!)
4. Process and mechanism to exclude from certain processing (see IAR)

See appendices 2.3 Processes and 2.7 Information Asset Register.

5 Subject Access Requests

The process to handle requests on the data you hold needs to be efficient to meet the response time constraints (reducing to a month) so might look at *create a web interface* so they can update it themselves.

See appendix 2.3 Processes.

6 Lawful basis for Processing

Primarily consent, so see IAR above for “How you acquired the data”, for which you may need extra fields for where and how that consent can be demonstrated (where is the evidence of the consent)

See appendix 2.7 Information Asset Register

7 Consent

As above, ensure you have fields for recording the consent and processes for its collection and management.

See appendices 2.2 Consent Statement and 2.7 Information Asset Register.

8 Children

Consider if data may refer to children, (retention periods are a lot longer/ start event is deferred) in which case may need to *add field for age* and then extend the consent record to *indicate who provided the consent.*

There will then need to be a process to check when they become responsible themselves.

See appendix 2.7 Information Asset Register and Recital 38.

9 Date Breaches

Need to document procedures for the detection, reporting, and investigation of data breaches. It may be that your business is one which is required to notify ICO. Have a procedure for assessing the significance of a data breach.

See appendices 2.5 Incident Response Plan.

10 DP by Design and Impact Assessment

It is good practice to assess your vulnerability to failure of business data and processes, but some conditions require a formal assessment of the impact of what you do itself.

See appendix 2.7 Asset Register table 3: Risk Assessment.

11 DPO

Consider rules to see if you need a formal Data Protection Officer or just add it as another hat to someone “suitable” but they do need to take it seriously and have the clout to enforce compliance.

See Article 37.1, this is outside of the scope of this document although further information is available from Tranlowe.

12 International

If your organisation operates in more than one EU member state, you should determine your lead data protection supervisory authority. If you only operate in this country then don’t worry, it is the ICO, otherwise work out where your head office really is, see the Article 29 working party guidance currently at http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

International operations are outside the scope of this document.