Awareness

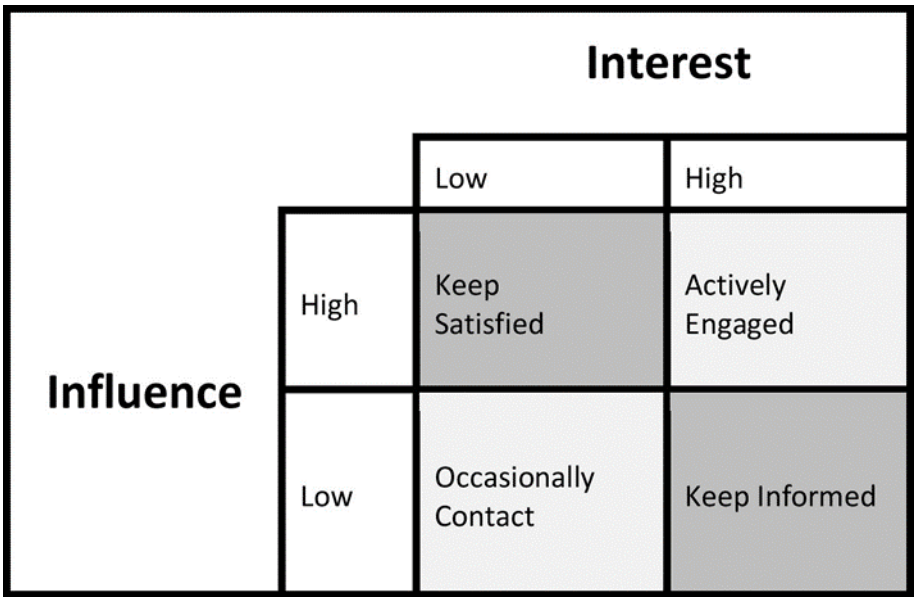
Contents

Awareness

GDPR is going to affect people in different ways. In many cases, there are going to be competing commitments. A good example is where a Controller needs to find the right balance between those who view personal data as a commodity which can be monetized, and those who see personal data as sacrosanct. In this Chapter, we are going do a deep dive into how we create compelling awareness. We will examine different stakeholders to get a sense of how these various groups feel about GDPR. The analysis in this book will be generic, but I would encourage you to conduct a similar exercise within your organisation, tailoring the analysis accordingly. Once you have this analysis, it can be converted into a communication plan. This plan will be an invaluable tool, aiding Data Protection Practitioners in customising their GDPR programmes and in particular how the programme content is communicated efficaciously.

Stakeholder Analysis

A particularly useful way to analyse is to assign stakeholders into a power-impact grid, shown in the table below. This analysis enables you to identify stakeholders regarding interest (i.e., how much they want to know what you are doing) and influence (i.e., how much power they have to affect your programme). Once the type of stakeholder is identified, a strategy for keeping the stakeholder onside can be formulated. For example, a high impact, high influence stakeholder will need to be kept in the loop and positively engaged as they could cause significant disruption to a programme. However, in contrast, low power, low-interest stakeholder is someone who still needs to know what is going on but is likely only to require occasional contact. Before using the power-impact grid, a Practitioner must identify their stakeholders. I recommend listing all stakeholders, as many as you can think of and then getting others to provide their input too. It is common to feel 'such and such won't be interested' and then take a decision not to include this stakeholder in your grid. I would caution against this approach. Stakeholder positions in a power-impact grid can and do, change over time. A CFO who was initially disinterested could suddenly become very interested if a significant sum of money, say to implement new technology, is requested. A newly promoted stakeholder could also have increased influence and will now need to be engaged differently. As a result of the inevitability of such changes, the Practitioner must periodically review stakeholder analysis because knowing which stakeholders are likely to throw you curveballs will give you the best chance of heading off their concerns, ideally before they even realised they had an interest in the first place. So, let us have a look at some of the key stakeholders from the perspective of the Data Protection Practitioner, to give you a feel who will need occasional contact and who will need active engagement. Some people find it practical to look at stakeholders from the perspective of those internal to your organisation and those external, but I prefer to keep them all together because stakeholders interact and it is a lot easier to assess those dependencies if stakeholders are kept together.



Power-Impact Grid, Office of Government Commerce, 2003

Data Subjects

Arguably, in terms of GDPR, the Data Subject is the most crucial Stakeholder. GDPR gives the Data Subject significantly more influence over how an organisation can process their data. It should be anticipated, given media attention surrounding the regulation, and recent data breaches, interest will be high - at least initially. When it becomes common knowledge, the charges relating to Subject Access Requests have been removed, and that a request can now be made in electronic form (**Article 12**: Transparent information, communication and modalities for the exercise of the rights of the Data Subject, Para (3).), the interest of Data Subjects to find out what data organisations hold is assessed to be very high. Stakeholder Group: Actively Engaged.

Privacy Groups

Privacy Groups have been battling on behalf of Data Subjects for years to enhance data protection regulation. In some cases, privacy groups have supported plaintiffs via funding, legal advice, research and creating media awareness of a particular issue. For the most part, interest and influence on a specific organisation are assessed to be low. Organisations should be mindful, however, should Data Subject's rights be neglected, interest will increase. Stakeholder Group: Occasionally Contact.

The Media

Media interest in GDPR will ebb and flow, the key for any organisation is to manage their reputation. Getting Data Protection wrong, either by failing to uphold Data Subject's rights or, suffering a security breach, is likely to attract adverse media attention. Companies do not enjoy the Right to be Forgotten (**Article 17**: Right to erasure ('right to be forgotten')) so once a breach has made it online, it is going to be there forever! Stakeholder Group: Keep Satisfied.

Hackers & Hacktivists

Certain types of hackers are incredibly interested in personal data as they use it to commit identity theft and other forms of fraud. The more intimate the data held; the more interested hackers would be in your organisation. The less secure your organisation, the more interesting an organisation's systems will be to the Hacker. Hacktivists have a slightly different motivation; they are more interested in causing damage to organisations because they disagree with specific practices. It maybe they believe an organisation is a massive polluter or are overcharging for life-saving pharmaceuticals or have just caused millions to lose their homes. Hacktivists will be keen to embarrass and disrupt. The influence of hackers and hacktivists will depend on their capability to attack and your organisation's capacity to defend itself. Stakeholder Group: Keep Satisfied.

Supervisory Authority

The Supervisory Authority will have a keen interest in organisations who are not upholding the rights of Data Subjects, so it would be wise to keep them in the low-interest box on the power-impact grid as GDPR gives supervisory authorities much greater powers than they have previously enjoyed. A Supervisory Authority can mandate an audit of your organisation, compel corrective action and in the worst-case scenario impose significant fines. The Supervisory Authority is a stakeholder whereby if their position on the grid changed from a low to high interest in your organisation, active engagement is going to require much effort. I would recommend keeping to the default. Stakeholder Group (default): Keep Satisfied.

Member States Courts / Judiciary

Naturally, the judiciary will always be a stakeholder when legislative instruments are involved. GDPR gives Data Subjects a number of rights such as the right to a judicial remedy against a Controller, a Processor (**Article 79**: Right to an effective judicial remedy against a controller or processor) and even the Supervisory Authority (**Article 78**: Right to an effective judicial remedy against a supervisory authority). A Data Subject also has the right to receive compensation from a Controller or Processor (**Article 82**: Right to compensation and liability). Therefore, the optimal place for this stakeholder is low interest and low influence, but where a Data Subject decides to seek a judicial remedy, interest and influence may become high very quickly. Stakeholder Group: Occasionally Contact.

Organisational Senior Management & The Board

To successfully implement GDPR, senior organisational management and the Board must be interested as ultimately, they are accountable (**Article 5**: Principles relating to processing of personal data) for ensuring their organisation can demonstrate compliance with the Regulation. Concurrently, Senior Management has the most influence within the company; they will have the final say on the allocation of resources required for a successful programme. It may be challenging to maintain their interest and benefit from their influence, as you jostle for priority against the organisation's other commitments, but keep at it, as a failure to engage this stakeholder group will lead to disaster! Stakeholder Group: Actively Engage.

Committees

Senior Management, certainly in larger organisations, often establishes committees to oversee different aspects of governance. Examples are Audit, Risk, Compliance, Operations and, more common in recent years, Technology committees. In each committee described above, GDPR is

going to become part of the agenda. The minutes and reports generated by these committees will also form part of the evidence required to demonstrate compliance. Stakeholder Group: Keep Informed.

Chief Risk Officer (CRO)

Risk is a common theme throughout GDPR. A Controller is required to take into account the risks (**Article 24**: Responsibility of the Controller) to the rights and freedoms of Data Subjects and, in doing so, ensure appropriate technical and organisational measures are in place. These measures must be sufficient to demonstrate that processing is performed in accordance with the requirements of GDPR. Given the material impacts a breach of Data Subject's rights could have on an organisation, the CRO will be interested in GDPR and will be a crucial ally in terms of ensuring risks are adequately mitigated. Stakeholder Group: Keep Informed.

Chief Information Security Officer (CISO)

Security is also a common theme throughout GDPR. Both Controllers and Processors are required to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk to the rights and freedoms of Data Subjects. Depending on where the CISO sits in the hierarchical structure of an organisation will have an impact on how they respond to GDPR. If they sit within IT, for example, their objectivity could be compromised due to conflicts of interest with their boss the CIO. However, if the CISO sits outside of technology, they should be a key ally. Nurturing this relationship will be critical. Stakeholder Group: Actively Engage.

Chief Information Officer (CIO) / Head of Technology

From an operational perspective the CIO is, without doubt, a critical internal stakeholder and should have a high interest in GDPR. The CIO typically controls the technology budget and therefore holds much influence in regards to applications and infrastructure where personal data will be processed. It is vital to understand the motivations of the CIO as they could be under significant pressure to keep IT costs down and are an increased regulatory burden could be perceived as an unwanted headache. Stakeholder Group: Actively Engage.

Head of Legal

GDPR is going to make the Legal department busy. Every contract with a Processor is going to require a review and in a percentage of cases will need significant renegotiation. In the event a contract is not in place, work will need to be done to get terms in place as GDPR now makes it a requirement (**Article 28(3):** Processor). Additionally, and now fees can no longer be charged for subject access requests, an increased likelihood exists the Legal department will support higher volumes of requests. This increased effort will likely manifest in terms of advising business units on legal risks associated with disclosure, redaction and applicable case law.

Head of HR

Human Resources are big consumers of personal data and not only about employees. HR stores data on candidates, former employees, next of kin, beneficiaries (e.g., pensions or death-in-service payments) and in some cases dependents (e.g., for the provision of private family healthcare). All this data must be processed in a manner which upholds the rights of the Data Subjects (Data Protection - The Employment Practices Code, ICO, Nov 2011). The Head of HR will still need to be

interested in Data Protection after GDPR and will have a lot of influence relating to how HR personal data is processed. In recent years, there has been a trend in HR to outsource HR tasks such as recruiting, payroll, employee engagement, learning & development, background screening. Each of these outsourced processing activities must have a contract in place under GDPR. Such a contract must include a requirement to ensure data is processed securely and that a Processor cooperates in demonstrating compliance with GDPR. As HR manage processes relating to candidates, employees and former employees, it is important the Head of HR fully understands these groups are still considered Data Subjects. HR is typically a focal point for Subject Access Requests and as such, HR will need to be on the ball in terms of responding the requests from Data Subjects (e.g. A candidate is entitled to request interview notes if they are not successful after a job interview). Stakeholder Group: Actively Engage.

Head of Marketing

Whichever level of sophistication, marketing is going to be … let's say … interesting! Not only must marketers comply with GDPR, but they must also comply with PECR (The Privacy and Electronic Communications (EC Directive) Regulations 2003). Marketers deal with massive volumes of personal data, so there is a high likelihood a lot of work will be required to ensure GDPR compliance. We are already seeing some initial reaction from organisations deleting marketing databases (Wetherspoons deletes entire email marketing database (http://www.decisionmarketing.co.uk/news/wetherspoons-deletes-entire-email-marketing-database, 27 June 2017)) and companies fined for distributing emails to customers without consent (Flybe Limited ICO Penalty Notice: https://ico.org.uk/media/action-weve-taken/mpns/2013731/mpn-flybe-limited-20170320.pdf, 20 March 2017)). Ironically in one case, a cited reason for a mass email was to comply with GDPR (Honda Motor Europe Limited ICO Penalty Notice: https://ico.org.uk/media/action-weve-taken/mpns/2013732/mpn-honda-europe-20170320.pdf, 20 March 2017)). Stakeholder Group: Actively Engage.

End Users

For GDPR, end users are those employees, contractors and others who are working directly with personal data. They could be a member of an operations team processing a delivery order, a member of an HR team processing candidate CVs / application forms or, a member of a sales team chasing leads. These days it will be pretty much everyone in your organisation with maybe a few exceptions (e.g., cleaners, maintenance engineers). End Users will often be in direct contact with Data Subjects, and under GDPR a subject access request can be made to anyone within an organisation (including the cleaner!) so End Users will all need to know what they must do to comply. Stakeholder Group: Keep Informed.

Third Parties & Suppliers

Outsourced service providers should be interested because it is going to be a lot more challenging for a buyer to justify choosing an organisation to process their data which has already been breached over an organisation that has a strong data protection culture. Third party suppliers who can demonstrate they are taking GDPR seriously will be in a much better position to influence purchasing decisions. In the case of existing suppliers, there will be existing risk which will require active management and the more suppliers processing personal data, the higher the risk. Stakeholder Group: Actively Engage.

Communications Planning

Understanding stakeholders, and identifying an appropriate engagement strategy, is all well and good at a high level. Sooner or later, you are going to have to follow through and start communicating! Now, you may work in a large multinational with a large internal communications team and, an even larger marketing and Public Relations (PR) team. If that is you, then there is every possibility you can get this work done for you, and I would encourage you to go down this route first. If this is not you, or those teams cannot spare anyone to support you, it is highly likely you are going to need to develop a communications plan.

Communications planning (Project Management, Watt A, 2016. ShareAlike 4.0 (CC BY-SA 4.0)) is about keeping everybody informed. The communications planning process concerns defining the types of information you will deliver, who will receive it, the format for communicating it, and the timing of its release and distribution. It is likely 90% of a Practitioner's role will be spent on communication, so it is important to make sure everybody gets the right message at the right time. For those of you who like a template, I have included one at the end of this section, but before we get to that, a good communication plan will consist of the following elements:

1. Identify stakeholders and their expectations
2. Identify necessary communication to satisfy stakeholder expectations
3. Determine frequency of communications
4. Determine message channels
5. Confirm who will communicate messages
6. Document items (e.g., templates, formats, documents)
7. Measure Engagement

As we have already covered point one, let us look at points two to six in a little more detail:

Necessary communication

To determine what is required communication you will need to set out communication goals (i.e., what do you want to communicate). Some useful communications goals for a Data Protection programme could be:

1. Communication of roles and responsibilities to affected employees
2. Communication of changes in deadlines for SARs (30days)
3. Communication of new mandatory breach notification deadline (72hours)
4. Communication of new policy requirements

Each of these goals could be broken down further by the audience for example. Remember, what is necessary communication for one person, can be too much or too little for another person. One rule of thumb I have found works well is the more senior a person is in an organisation, the shorter the communication. Take, for example, creating a slide deck. For a relatively junior or broad audience, having a number of slides may be appropriate, for the Board, you should ideally be looking at no more than two – and probably more realistically – just one.

If you are not getting the expected response back from your email communication, try the Bottom Line Up Front (BLUF) technique. Write the email as you usually would, then move the last line, your request for action, to the top. Always include words to the effect "would it be possible to get this back to me by…?" Most people writing a business email, do so in the same way they communicate verbally. The email explains (often at length) the background to a situation, presents courses of action and only then, after many paragraphs of supporting analysis, will there be a call to action. The trouble is when busy people see long emails; they often put it in the 'I will read that properly later' folder…which eventually becomes the 'never going to read' folder. If you put the call to action and a deadline at the top of the email, it is more likely you will get a response. If you put a suggested deadline, you will help the person in prioritising when the work needs to be completed.

Communication should also be appropriate to your intended objective. If you want a decision from someone, then make that explicitly clear. Don't go into the Boardroom saying you have identified a requirement for an eDiscovery tool and it costs £150k and then walk out of there without first ensuring you have explicitly asked the Board for a funding decision.

Frequency & Channels

Timing is always going to be important when it comes to communication. In most organisations which have a committee structure, there will be deadlines before standing meetings when materials must be submitted. These deadlines are so committee members can read the meeting pack before the meeting (that is the idea anyway!). When planning your programme's communications, you must take this into account so you can provide stakeholders with the most current information. In terms of written reports, keep to one document which can be expanded/contracted, dependent on the audience. In your master document, avoid complex formatting, this way you can transfer material into the dozens of other people's templates with a lot less effort.

EXAMPLE

Computer Based Training is an excellent communication channel for interactive information. As are Town Halls and Workshops.

In terms of channels, there are too many to list out. So many it can become overwhelming when you think of just how many ways a person can now interact with others. To keep things simple, try and group the information you wish to communicate into static, fluid, and interactive and then pick a channel suitable for such information. Static data is items unlikely to change often such as a privacy notice. Fluid information is likely to change over the course of time, such as a project progress report. Interactive information, as the name suggests, will vary based on interaction with an audience such as a social media site.

The Messenger

Most people will tell you, if they are honest, they prioritise reading and responding to emails coming from their boss or someone significantly senior like the CEO. This behaviour is of course understandable. A line manager will conduct appraisals and so will assess team members on how well they have performed against tasks they have set. It is likely such assessment will also have a direct impact on any pay rises, promotions or bonuses. Understanding who motivates a person to action is just as important as the message containing the call to action. A word of caution when asking others to communicate on your behalf, be aware they will need guidance. Guidance can include key talking points, frequently asked questions, who can help with more difficult questions and so on. Don't just draft them an email and leave them to it!

Documentation

In addition to the template mentioned at the beginning of this section, the following items should be documented and maintained as part of your communication plan:

1. Communication Plan!
2. Branded Templates (for consistency)
3. Content of emails
4. Wiki Site / Intranet Portal
5. Posters
6. Press Releases
7. Learning Objectives for Training
8. FAQs
9. Guidelines for Line Managers communicating to their teams
10. Policy for communication with external organisations (e.g., Media)
11. Policy for communication with customers and general public

Measure Engagement

Communication is not one way; it requires some form of response. Often inexperienced Practitioners are guilty of thinking sending an email, telling everybody what they must be doing, is communication. These missives are not communication, it is dissemination and is likely to be highly ineffective if the person receiving the information is not a willing participant. An effective communication plan will require multiple forms of measurement to ascertain how successful communication has been in achieving the intended goals.

EXAMPLE

A communication objective is to inform employees of new SAR deadlines via e-Learning. To measure success a question is included in a test at the end. e.g.: Subject Access Requests must be answered in:

A - 40 days

B- 30 days

C- Take as long as you need to be thorough

Raising awareness can be an absolute minefield. If a Practitioner gets communication right, it will make their lives significantly easier. If on the other hand, communication is weak, it can break a programme. Before sending out missives or designing posters, document your communication plan and ask colleagues to sanity check the content.

Communications Plan Template

Communication Plan (Version x.x)					
Programme Nam e: General Data Protection Awareness					
Comms Plan Owner: *{Insert Name]*					
Stakeholder Analysis					
Name	**Role**	**Engagement**			
Communication Objectives					
Ser.	**Objective**	**Talking Points**			
Plan					
Issue Date	**Owner**	**Audience**	**Channel**	**Frequency**	**Location of Materials**
Notes:					

Awareness through Learning

Not hearing is not as good as hearing, hearing is not as good as seeing, seeing is not as good as knowing, knowing is not as good as acting; true learning continues until it is put into action (Xunzi, Xun Kuang, circa 260BCE). Wise words that have stood the test of time. A wise Practitioner should also incorporate this ancient philosophy in their awareness programme. By combining effective and

appropriate learning activities into your awareness programme, there will be a significant increase in your audience's engagement levels. The essential ingredients being effective and appropriate. Learning activities are often executed poorly with a little forethought in terms of the learning process. A typical approach is to look at a topic, add some slides covering the relevant parts and then getting participants in a room in an event often referred to as 'Death by PowerPoint'. Participants are then asked to sign a register for the audit trail and sent off into the world to apply their 'knowledge'. Practitioners often fail to incorporate any pedagogical steps. What the Practitioner should try aim to achieve is for those in scope of learning activities to become unconsciously competent in art and science of data protection. This state of being is where your employees don't consciously think about ensuring something is compliant with GDPR, but do it as an integral part of their duties. A word of caution, as people become consciously competent, there is a tendency for people to forget why they are doing something in a certain way or as new staff join the organisation, the reason behind a certain practice may not be passed on as part of any induction training. It is therefore critical the conscious competency learning framework is seen as cyclical, with practitioners understanding people can regress from consciously competent back to unconsciously incompetent, and any of the stages in-between.

1. UNCONSCIOUS INCOMPETENT You are **not** aware of a skill and your lack of competency	**4. UNCONSCIOUS COMPETENT** You are able to use a skill without thinking about it
2. CONSCIOUS INCOMPETENT You are aware of a skill and your lack of competency	**3. CONSCIOUS COMPETENT** You are able to use a skill but it takes effort

Conscious Competence Learning Framework (The Empathic Communicator. Howell, W.S., 1982)

Stages Of Learning

Unless you have a machine such as the one used in the Matrix Trilogy (excellent films by the way!), no one becomes an expert in anything overnight. A student goes on a journey to become competent and then onto mastering their chosen speciality. As a Zen Practitioner you are already there but how do you bring everybody else with you on the journey? an excellent way to do this is to customise training according to the different stages of learning. To create an effective training programme for your data protection programme, it is important to understand the stages of learning and how they can be applied. While I will list them, they should not be viewed hierarchically (i.e., you should use a stage appropriate to your intended objective).

Another factor to consider is the availability of resources. In a corporate environment, you will be competing with many other people when it comes to getting employees to participate in training, so it is important to get the best bang for your buck.

The learning stages (A Taxonomy for Learning, Teaching, and Assessing: Pearson New International Edition: A Revision of Bloom's Taxonomy of Educational Objectives, Abridged Edition. Anderson L et al., 2013) are:

1. Remember: Recognising and recalling facts
2. Understand: Understanding what facts mean
3. Apply: Applying the facts, rules, concepts, and ideas
4. Analyse: Breaking down information into components
5. Evaluate: Judging the value of information or ideas
6. Create: Combining parts to make a new whole.

Let's look at how this could be applied to a Data Protection programme training programme:

Learning Stage	Learning Objective	Audience
Remember	**Recall the six GDPR principles**	**All staff**
Understand	**Paraphrase the Right to Portability**	**IT Developer**
Apply	**Calculate the cost of an Administrative Fine of 4% of gross annual turnover**	**Risk Manager**
Analyse	**Categorise business processes into those in and out of GDPR scope**	**Process Owner**
Evaluate	**Assess the risks to a processing activity**	**Department Head**
Create	**Create an updated procedure for dealing with employee related Subject Access Requests (SARs).**	**HR Manager**

Bloom's Revised Taxonomy Applied to Data Protection

While this is a small snapshot of potential learning objectives, there are countless more. Once you have identified the most appropriate learning objectives for your programme, you then need to plan the learning activity to support the learning. Luckily, teaching is a mature profession, and the most commonly used tool is the lesson plan.

The Lesson Plan

A lesson plan's primary purpose is to support an educator in the delivery of a discrete learning activity. It places a structure around the activity in a similar way a communication plan or project plan does for communications and projects. The fundamental components are as follows:

1. Setting Learning Objectives: what are we trying to teach
2. Preliminaries: what is required to meet the objectives
3. Introduction: setting the scene
4. Learning Stages: breaking learning into manageable chunks
5. Guided Practice: supervising the application of knowledge
6. Review: confirm assimilation of knowledge
7. Consolidation: taking the learning back out into the workplace

Learning Objectives

In the stages of learning section, we touched upon learning objectives and how they relate to the different learning stages. A good objective will usually have a verb-noun pair of which an output must exist. The output must exist so the learning objective can be confirmed as being achieved by the learner, through evidence-based assessment. If a learning objective cannot be confirmed through evidence-based assessment, it is not a learning objective!

EXAMPLE

Categorise business processes into those in and out of GDPR scope.

Preliminaries

Before any instruction can take place, there is a certain amount of preparatory work. This work could be as simple as making sure there is a room with enough seats and chairs; through to printing handouts; to more complex preparations such as building an IT laboratory. If you are planning to use multimedia (e.g., PowerPoint) an instructor must, at a minimum, proofread slides, check projectors etc. are working and, sit in the seats of the participant to verify they can see the material. Rehearsing also comes under the prelims banner. As you become more competent in the material, you may not need to rehearse as much but whenever delivering material for the first time (even as an expert), do a dry run before unleashing the material on your real audience. Often, learning in a commercial environment is not going to be classroom based. There are so many different ways. The learning could be computer-based, via video conferencing or even one-to-one at a learner's desk. Whichever location, the basic tenet is proper planning and preparation will prevent poor performance!

Setting The Scene

Once you have rehearsed, set up your learning environment and are now face-to-face with those you intend to instruct, you now need to set the scene and explain why they are giving up their day jobs to attend your training. The introduction must, therefore, include the following components:

1. Preamble: how did we get to now
2. The challenge: what do we need to achieve
3. The learning objectives: how are we going to get there
4. Question policy: how can people ask for help/clarification

EXAMPLE

As we learned in a previous session, our organisation is required to demonstrate the personal data we hold is processed in accordance with GDPR. To do that we must identify which processes are in scope of GDPR.

As such, the objective of this session is to teach participants to categorise business processes into those in and out of GDPR scope.

The material may raise questions so, in order to get through the material efficiently, we will have Q&A points at each stage. If you have an urgent question, please let me know.

Learning Stages

This is where the meat of the instruction takes place. If you are combining multiple learning objectives into one lesson, each objective could be considered a learning stage. Each stage has the following component:

1. State the theory/concept
2. Explain the theory in context
3. Discuss a scenario
4. Ask and answer questions

EXAMPLE

A processing activity will be in the scope of GDPR is the process involves processing of personal data. Personal Data is [put a definition on slide]. Let's look at the following three scenarios.

For each are the processes in or out of scope and why?

Scenario 1: [use slide] Processing a loan application. In scope processing involves personal data of applicants.

Scenario 2: [use slide] Producing Balance Sheet. Out-of-scope as does not involve personal data.

Scenario 3: [Use slide] Monitoring Logs of Customer portal. Discuss what could bring this process into scope.

If the lesson is practical, such as training someone how to complete a Data Protection Impact Assessment (DPIA) the following approach should be used:

1. Explain the task
2. Demonstrate the task
3. Get participants to copy the task under supervision
4. Get participants to practice the task

When it comes to questions, a useful technique is to Pose, Pause, Pounce. Ask the whole group the question, pause and read the group's body language, and then pounce on someone you think will (or won't) know. Avoid singling a person out and then asking the question, as the rest of the group will switch off. Another good tip is to ask the rest of the group then whether they think the person is correct and ask the group why. The more interaction throughout the learning stages, the more the concepts will be assimilated! In some cases, you will not know the answer (or you have forgotten). The one thing you must never do – don't bluff. If you do not know the answer, explain you will check the regulation and get back to them with a definitive answer.

Guided Practice

This concept is more appropriate for practical tasks over theory and in workplace learning, there should be lots of opportunities to practice. A good way to carry out guided practice is to create a case study. Get participants to split into smaller groups and give participants a number of questions to answer.

EXAMPLE

The HR department of Acme Ltd need assisting in identifying processes involving personal data. In your groups identify ten processes likely to include personal data. For each process what types of personal data are likely to be involved.

Review & Confirmation

This is where all the learning is summarised, participants ask final questions, and finally, the instructor confirms the learning objective has been achieved. This confirmation can be by a Q&A session or a short-written test or an exercise. Whichever option is chosen the instructor needs to ensure the learning objective has been achieved by all participants. The Review section is also a useful time for the instructor to make a note of any questions that could not be answered and point participants in the direction of helpful reference material (e.g., an Intranet portal). It is also helpful to provide contact details as sometimes people are embarrassed to ask the 'stupid' question in front of their peers or a concept suddenly makes sense when they apply it for real and then results in questions they did not have during the course!

Objective: Recall the Six GDPR Principles

Confirmation: Participants will be asked to name a principle at random. Other participants will confirm the principle is correct. Alternatively, Instructor will state a principle and participants must confirm if the principle is correct.

Consolidation

No workplace learning should stop at the classroom; learning needs to be incorporated into day-to-day operational activities. As such, if you are integrating learning activities into your data protection programme, you should catch up with your participants and find out how the learning has helped (or hindered). Often feedback forms are sent out the same day as the course ends, which is pretty useless as how will the instructor know if the concepts are understood until the learning is applied. When seeking feedback, give it at least a couple of weeks! Awareness through learning, in my humble opinion, is the most efficient way of getting a message across to an audience. It is an especially effective medium where the message requires follow-on, and often, continuous application of the content – long after the learning activity has finished.

Lesson Plan Template

Lesson Plan (Version X.X)		
Lesson Name: e.g. Data Protection Impact Analysis		
Instructor: [Insert Name]		
Previous Leaning Activity: e.g. DPIA Theory		
Preliminaries		
Resources		
Location & Equipment		
Introduction		
Preamble		
Challenge		
Learning Objectives		
Question Policy		
Lesson Stages		
Stage	**Content**	**Notes**
1		
2		
3		
4		
5		
Review		
Final Confirmation		
Recap Objectives		
Summary & Look Forward		