Data Protection Essentials

The General Data Protection Regulation
(And more)

CIM
The Chartered Institute of Marketing

INTRODUCTIONS

- Mike Holland
  - Account Director, OlsenMetrix Marketing.
  - Chartered Marketer, Fellow of the Chartered Institute of Marketing, Member of the Chartered Institute of Public Relations.
  - Member of the Data Protection Network.
  - 35 years in marketing and PR.

DISCLAIMER

- Today's presentation is based on my understanding of GDPR.
- I have taken all reasonable care in preparing this presentation but I am not a lawyer and nothing in this presentation should be taken as being legal advice.
- Neither I nor CIM can take responsibility for the consequences of you implementing any of the suggestions made in this presentation.

ACKNOWLEDGEMENTS

- Data taken from:
  - Chartered Institute of Marketing.
  - Veale Wasbrough Vizards (Serena Tierney).
  - Fieldfisher (Kuan Hon).
  - Direct Marketing Association.
  - Data Protection Network.
  - Information Commissioner's Office.

- Cartoons taken from:
  - Office of the Privacy Commissioner of Canada.

WHAT IS THE GDPR?

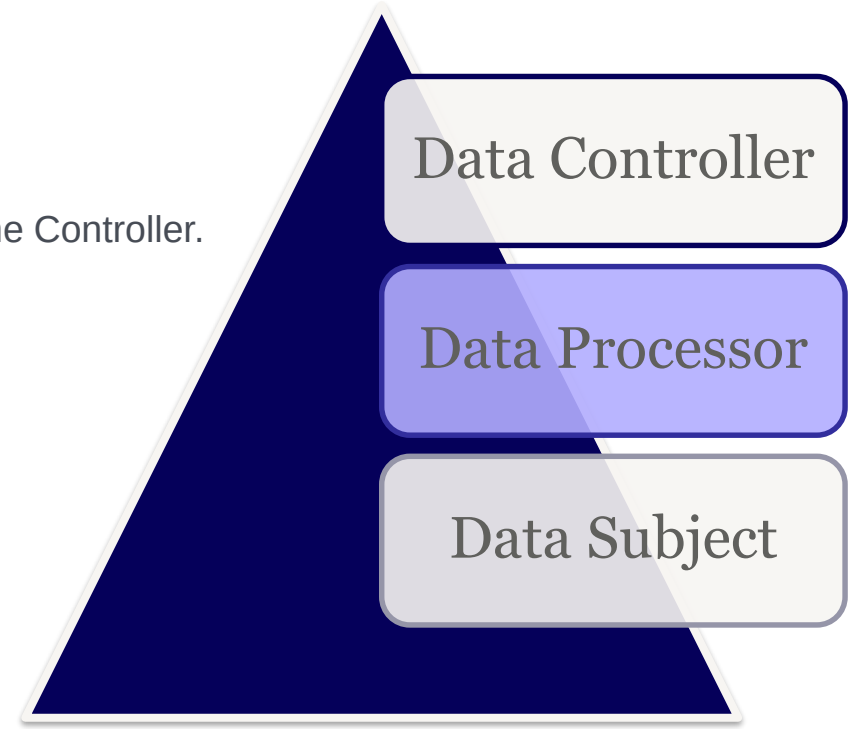
- The (European) General Data Protection Regulation.
- Comes into effect across the EU on 25 May 2018.
- Replaces existing EU and UK data protection law.
- Will be enforced in the UK by the Information Commissioner's Office (ICO).
- Will continue in force even after the UK leaves the EU.
- Being translated into UK law through the Data Protection Bill.
  - Committee stage in House of Lords November 2017
- Breaches can result in huge fines –
  - Up to 4% of turnover or €20 million.

GDPR PRINCIPLES

- It is **not** about database marketing and emails.
- It **is** about how organisations obtain, store and use personal information.
- It will: *"…enable people to better control their personal data. At the same time modernised and unified rules will allow businesses to make the most of the opportunities of the Digital Single Market by cutting red tape and benefiting from reinforced consumer trust."*
- It is 'technology neutral' – it is not about computers and emails, it is about principles.
  - It therefore covers files held on paper, the content of your filing cabinet, the contact list on your phone, telephone calls, direct mail – as well as computers and emails!
- People don't trust business or government with their personal data.
- GDPR aims to establish trust between citizens and data users.

DATA HIERARCHY

- Data Controller
  - Determines the purpose and manner in which personal data is processed.
- Data Processor:
  - Third party processing data on behalf of the Controller.
- Data Subject:
  - An individual subject of personal data.



DATA AND DATA PROCESSING

- Data is not only collected from people telling us things. It can be:
  - Observed by tracking people online or by smart devices.
  - Derived from combining other data sets.
  - Inferred by using algorithms (or humans) to analyse a variety of data, such as social media, location data and records of purchases in order to profile people - for example in terms of their credit risk, state of health or suitability for a job.
- If you do anything with the data which you collect or store you are ‘processing’ it
  - And if you’re not doing anything with it – why did you collect it?

WHAT IS PERSONAL DATA?

- GDPR is concerned with ‘personal data’ – but what is ‘personal data’?
- Anything which identifies an individual, or can be associated with an individual, is personal data.
- If business email addresses or IP addresses are linked to an individual they are ‘personal data’ and therefore subject to all the same protections as consumers’ data.
    - For example – the email address ‘joe.smith@xyz-company.co.uk’ is personal data because it identifies Joe Smith as being associated with xyz-company.

WHERE ARE WE AT RISK?

- HR/personnel/payroll.
- Marketing and sales.
- And other places you may not think of!

RISKS – HR/PERSONNEL/PAYROLL

- Basic employee data – name, address, age, job title, next of kin, salary, etc.
- Bank account details for payroll processing.
- Tax details for payroll processing – benefits, family circumstances, total income, etc.
- Appraisals.
- Disciplinary records.
- CVs and interview notes – successful and unsuccessful candidates (and their contact details).
- Medical details.
- Criminal records.
- Trade union participation.

RISKS – MARKETING AND SALES

- Customer data – name, address, age, etc.
- Email address and IP address.
- ‘Profiling’ information – employment, income, time at current address, credit score, etc.
- Bank account details.
- Purchase history.
- Payment history.
- Delivery records.
- Media lists.
- ‘Personalisation’ data collected by sales force (birthdate, children’s names, etc).

- *Considerations are different for ‘business to business’ and ’business to consumer’ companies – but even B2B companies need to give thought to all the above.*
- *Note that partnerships and sole traders are ‘consumers’ in law.*

RISKS – OTHER AREAS

- Accident record book.
- Reception, post room – who else handles and uses data?
- Data shared with third parties (eg, delivery contractor).
- Supplier data.
- ‘Personal’ address books, customer data, etc.
- Email systems.

… AND THERE'S MORE …

- There are specific additional requirements around collecting, storing and using data about children.
- Seeking to identify website visitors without consent is probably unlawful – adding a line about this to your 'cookie warning' may not be enough.
- Gathering, recording and analysing data from social media may be unlawful.
- If data leaves the EU there must be specific policies and procedures in place.
- If you are using Google Analytics you should be aware that Google's Terms of Service say:
  - "You will have and abide by an appropriate privacy policy and will comply with all applicable laws, policies, and regulations relating to the collection of information from visitors. You must post a privacy policy and that privacy policy must provide notice of your use of cookies that are used to collect data. You must disclose the use of Google Analytics, and how it collects and processes data."

PERMISSIBLE PROCESSING

- For most companies there are four legal bases on which data can be collected, stored and used under GDPR:
  - Contractual – if you need the data to fulfil the contract (eg, a delivery address).
  - To fulfil legal obligations – for example, recording details of accidents on site or demonstrating compliance with regulations.
  - With the informed consent of people about whom data is collected, stored and used.
  - To pursue 'legitimate interests'.
    - This will permit collection and use of data for HR purposes or for prevention of crime.
    - It may also cover collection and use of customer details for marketing purposes *if certain conditions are met.*

- *The other bases for permissible processing are 'vital interests' (of the individual concerned) and 'public task'.*

WHAT IS A LEGITIMATE INTEREST?

- An interest is ‘legitimate’ if it is ‘necessary for achieving our commercial or business objectives’.
- Note that ‘necessary’ is not as stiff a test as, for example, ‘vital’ but neither is it as weak as ‘useful’, ‘reasonable’ or ‘desirable’.
- An easy test may be to ask “Is there another way of achieving the identified objective?”
  - If there is not, then the processing is necessary; or
  - If there is another way but it would require ‘disproportionate effort’, then we may still decide that the processing is necessary.

INFORMED CONSENT

- Where we are relying on ‘informed consent’ as the basis for collecting and storing data we must:
  - Collect only the data we need.
  - Tell people why we are collecting data.
  - Secure real ‘informed consent’ (which means they must positively agree to their data being collected – not simply fail to object).
  - Provide a clear statement of policy accessible to people whose data we are processing.
  - Use data only for the purposes for which we said we would use it or in ways that people would reasonably expect.
  - Secure repeat ‘informed consent’ at ‘reasonable intervals’ – so we cannot keep people on a database indefinitely without asking them to confirm their consent.
  - Inform people that they may opt out at the time that data is collected and during appropriate interactions thereafter, give them an easy way to opt out, and then ensure that the opt-out is acted upon.
  - Have procedures in place to record opt-outs in case of challenge and to screen new imported data.
  - Have and implement policies on data retention and destruction.

KEY REQUIREMENTS FOR COMPLIANT CONSENT

- ‘Informed’ – People must know what they are consenting to.
- ‘Positive’ – Pre-ticked boxes are invalid. People must give real consent. Not consenting must be given equal prominence when choices are offered.
- ‘Unbundled’ – Consent requests must be separate from other terms and conditions.
- ‘Granular’ – This is not actually a requirement – but good practice would be to give people control (wherever possible) over what types of communication they want (or do not want) to receive. This will help to avoid a ‘blanket opt out’. However, the choices must be clear and self-explanatory.
- ‘Documented’ – Keep records as to what people signed up to, when, where, how and what they were told at the time.

LEGITIMATE INTERESTS

- Direct marketing is specifically mentioned in GDPR as a ‘legitimate interest’ (in Recital 47).
- Where we are relying on ‘legitimate interest’ as the basis for collecting, storing and using data we must:
  - Carry out and document a ‘legitimate interest assessment’ which demonstrates that it is lawful to rely on ‘legitimate interest’.
  - Collect only the data we need.
  - Tell people whose data we are processing that we are doing so on the basis of a legitimate interest.
  - Provide a clear statement of policy accessible to people whose data we are processing.
  - Give people an easy way to ask to opt out – and then ensure that the request is acted upon.
  - Have procedures in place to record opt-outs.
  - Have and implement policies on data retention and destruction.

*Note: The GDPR says ‘the processing of personal data for direct marketing purposes **may** be regarded as carried out for a legitimate interest.’ We must still carry out a legitimate interest assessment.*

WHAT'S COMING NEXT?

- The e-Privacy Regulation.
- Originally intended to be implemented alongside GDPR.
- For a variety of reasons the e-Privacy Regulation has been delayed – but it has not gone away.
- 'Best guess' is that the regulation will be approved between October 2018 and April 2019.
    - This straddles the 29 March 2019 date which is technically 'Brexit Day', two years after the UK gave notice under Article 50 of the EU Treaty.
    - So, will the Regulation be 'imposed' on us as an EU member or need to be separately addressed by UK legislation? And if the latter, when?
    - Indications from government are that it will be imposed in UK law.

THE E-PRIVACY REGULATION

- Much of the e-Privacy Regulation is about the privacy of communications on the internet and other electronic services.
- However, it also covers direct marketing activity via electronic means.
- Currently regulated in the UK by the Privacy and Electronic Communications Regulation (PECR).
- PECR does not deal with the wider use of electronic communications today and will be further outdated by GDPR.
- The current draft e-Privacy Regulation is under negotiation in Europe and it is possible that some of the text may change.
- But we can predict the main requirements:
    - There will be no distinction between B2B and B2C personal data.
    - You will need ‘informed consent’ before you can contact people.
    - The ‘soft opt in’ principle will give some flexibility.
- The EU Parliament’s Committee on Civil Liberties, Justice and Home Affairs (LIBE) and full EU Parliament voted to approve amendments to the draft directive which confirm the above.
- The Council of Ministers has yet to vote on the issue.

SOFT OPT-IN

- ‘Soft opt-in’ allows you to assume consent for email marketing under the e-Privacy Regulation if:
  - You obtain electronic contact details during the sale of goods or services.
  - You use those details only to promote your own similar goods or services.
  - You give the customer the opportunity to easily opt-out at any time – so provide an ‘unsubscribe’ link in every mailing.
- Soft opt-in applies to all electronic channels – such as email, SMS, social media and instant messaging apps. However, you must tell the customer which channels you intend to use at the point of collecting the information.

If you do not have soft opt-in, you must obtain consent.

OTHER TECHNOLOGIES COVERED BY E-PRIVACY

- Telephone sales calls can still be made as long as the individual or organisation has not objected via TPS or CTPS.
  - We will have to provide caller line identification or a mandatory prefix (yet to be decided).
- Tracking technology.
  - Cookies, web beacons, hidden identifiers, device fingerprinting and any other technology that is developed to track the activity of the individual will need consent from the end user.
- Instant and social media messaging services (eg WhatsApp) and VOIP services (eg, Skype).
- Metadata such as numbers called, websites visited, geographical locations cannot be shared without consent.

PART 2

CIM
The Chartered Institute of Marketing

CONSENT, POLICIES AND PRIVACY NOTICES

- If we wish to rely on ‘legitimate interest’ we must inform people that we are processing their data on this basis and what the legitimate interest is.
  - It may be helpful to stress that the privacy rights of individuals were considered when the decision was made and to emphasise the benefits processing will provide to the individuals.
  - We must also inform people of their right to object to processing on these grounds – *we’ll return to this topic later.*
- Information provided to individuals about data processing (on whatever basis) must be explicit, clear and separate from other information.
  - It must also be appropriate to the individual and the circumstances.
  - ‘Multi level’ or ‘layered’ provision of information may be a sensible approach in most circumstances.

CONSENT, POLICIES AND PRIVACY NOTICES

- Privacy policies should:
  - Be presented at a time when it is relevant to people's decision whether to provide their personal data.
  - Use clear, straightforward language in a simple style that people will find easy to understand.
  - Avoid confusing terminology or legalistic language.
  - Be in the house style/brand tone of voice.
  - Be truthful – not offering choices that are misleading.
  - Be easy to find and consistent across multiple platforms.
  - Give full disclosure about what information is being collected and what is being done with it.

CONSENT, POLICIES AND PRIVACY NOTICES

- Privacy policies should:
  - Identify the data controller.
  - Specify what data you collect.
  - Specify how you collect data.
  - Explain why you collect the data and what you do with it.
  - Explain any profiling that you undertake with the data.
  - Say who, if anyone, you may pass the data to.
  - Specify the basis on which you collect data (contractual obligation, legitimate interest, etc). If you are relying on legitimate interests, explain what these are.
  - Explain the rights of individuals to object to data processing, to see what data you hold, etc.
  - Explain your data retention/destruction policy.
  - Explain the right of complaint to the ICO.
  - Provide assurances of data security.

CONSENT, POLICIES AND PRIVACY NOTICES

- Small businesses must keep a record of all ‘high risk’ data processing. Large businesses (more than 250 employees) must keep a record of all data processing.
- ‘High risk’ is sensitive data:
  - Medical records and financial data are ‘high risk’.
  - Home address and postcode are (probably) ‘low risk’.
  - Each data class needs to be assessed ‘on its merits’.
- We must have a clear policy, communicated to all relevant staff, about privacy and data security.
- We must have evidence that the policy is implemented.
- The policy must set out the organisational and technical measures used to protect privacy and ensure data security.
- We must be able to supply the policy and evidence on demand to the ICO.

DOWNLOADS AND RELATED ISSUES

- GDPR principle – collect only the data you need and use it for the purposes for which you said you would use it.
- You do not need to collect any data to permit something to be downloaded from a website.
- Consider instead:
  - Opt-in email to receive the ‘download’ and other related data.
  - Contractual obligation.

OBJECTIONS AND OPT-OUTS

- People have a right to object to our processing of their data and we have an obligation to tell them this at the time the data is collected or on ‘first contact’.
- We must remind them of their right to object at ‘reasonable’ intervals.
- We are obliged to consider and respond to each objection. We are not obliged to accept it.
    - In some cases, such as direct marketing, an objection from an individual to our processing of his/her data will override our legitimate interest.
    - In other cases, such as fraud prevention or computer security, an objection may not be enough to override our legitimate interest.
- We must have clear systems in place to handle objections. Processes must be clearly set out when we remind people of the right to object.
    - An objection to processing for direct marketing might be dealt with automatically by the individual through an unsubscribe link or online preference centre.
    - An objection to processing for HR purposes may need to be made in writing.
- Revoking consent should be as easy as giving consent – eg, if consent was given by tick box, then opting-out should be via a similar method.

OTHER INDIVIDUAL RIGHTS

- Individuals have a ‘right to be forgotten’ (a ‘right to erasure’) if we have no legitimate reason to continue holding their data.
- Individuals have a right to see what data we hold on them. We must provide this free of charge but can levy a fee representative of the actual cost of providing the data if requests are unreasonable or excessive.
- Individuals have a right to have any errors in the data we hold about them corrected when these are drawn to our attention.
- We must respond to requests within a month (maximum).
- We must provide the data in a ‘portable’ format - a structured, commonly used and machine readable form.
- We must take ‘reasonable care’ to ensure that the person to whom we give data is the individual we think it is!

DATA PROTECTION AND SECURITY

- We must store and process data in a manner that ensures ‘appropriate security’.
- Security must include protection against:
  - Unauthorised or unlawful access or processing
  - Accidental loss, destruction or damage.
- Security must include appropriate technical and organisational measures.
- A legitimate interest assessment should contain a section on the safeguards and controls (technical and organisational) that are in place to keep data secure.
- Where data is being processed on some basis other than legitimate interest a separate ‘privacy impact assessment’ should be carried out which, again, should contain a section on the safeguards and controls (technical and organisational) that are in place to keep data secure.

DATA BREACHES

- We must report certain types of data breach to the ICO and in some cases to the individuals affected.
  - We must report any breach of security leading to the “destruction, loss, alteration, unauthorised disclosure of, or access to, personal data”.
  - We must report if the breach is likely to have “significant detrimental effect on individuals” – for example, damage to reputation or financial loss.
  - Where the breach is likely to result in a “high risk to the rights and freedoms of individuals” we must notify those concerned directly.
  - The report must be made within 72 hours of discovery of breach.

ENFORCEMENT

- The ICO can levy fines of up to €20 million or 4 per cent of global turnover.
  - If you think you have been unjustly ‘convicted’ or the fine is excessive you can appeal to the courts.
- The law is the law …. but ….
  - The ICO is likely to give some time for new rules to ‘bed in’ – but officially there is no ‘grace period’.
  - The ICO has a policy of ‘helping to comply’ rather than moving straight to enforcement.
  - Initial ‘enforcement’ from the ICO is likely be a ‘notice to comply’.
  - The ICO’s first enforcement targets are likely to be big firms.

BEYOND ENFORCEMENT

- Fines from the ICO may be the least of your worries ….
  - In some cases, directors and executives may face prison sentences.
  - Reputational and business damage may be immense.
  - GDPR makes specific provisions for ‘class actions’ by data subjects.
  - The data controller is generally responsible – but data controllers may opt to sue data processors. And data subjects may sue either.

CONTRACTS

- There should be a contract between data controller and data processor.
- The contract should specify that the processor will at all times act only on the instructions of the controller.
- The contract should guarantee to both parties that the other is GDPR compliant.
- The contract should require the processor to comply with data security obligations equivalent to those imposed on the controller.
- The contract should set out what happens in the event of a breach of security.
- The contract should set out the processor's obligations for data retention and destruction.
- Ideally the contract should specify the mechanisms for exchange of data between the parties.
- Unless the contract specifies otherwise – whatever happens is the responsibility of the data controller!

THE END OF THE WORLD AS WE KNOW IT?

- GDPR and e-Privacy Regulation merely reinforce what we should be doing already.
- Data Protection Act 1998 and Privacy and Electronic Communications Regulations.
- The ICO recently:
  - Fined a small firm £60,000 after customer details were stolen because the firm held onto data for too long and did not protect it adequately.
  - Secured a criminal conviction against a charity worker for downloading data to his laptop.
  - Fined a data broker £80,000 for failing to tell people what is was doing with their data.
- A consumer group recently launched a £1 billion ‘class action’ against Google in the UK backed by a £15.5 million legal fund.
- The High Court recently permitted a group of Morrisons employees to launch a class action against the company after payroll and other details were leaked. The employee who leaked the data has already been jailed for eight years.

And that’s **before** GDPR comes into effect!

ACTION PLAN – DATA ASSESSMENT

- Appoint a ‘data protection officer’ - mandatory if you carry out large scale systematic monitoring of individuals (for example, online behaviour tracking) or carry out large scale processing of special categories of data (for example, data relating to criminal convictions and offences).
- Find all the data that you collect/hold/use. Explore every ‘nook and cranny’ of the business.
- Examine the data you have found. Is it necessary? If not, delete it.
- Try to group the data that you do need to keep into logical classes – eg ‘HR data’.
- What is the legal basis for you holding the data (eg, ‘legitimate interest’)?
- Can you apply that to all the data in the class? If not, consider splitting the class into sub-classes with the same legal basis.
- Where a class of data is presumed to be held on the basis of legitimate interest, conduct a legitimate interest assessment to see if this is valid.
    - If it is not, either find a different legal basis for holding the data – or, if none exists, delete it.

DATA PROTECTION OFFICER

- GDPR defines the Data Protection Officer's (DPO's) minimum tasks as:
  - Inform and advise the organisation and its employees about their obligations to comply with GDPR and other data protection laws.
  - Monitor compliance with GDPR and other data protection laws, manage internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
  - Be first point of contact for ICO and for individuals whose data is processed.
- You must ensure that the DPO:
  - Reports to the highest management level – ie board level.
  - Operates independently and is not dismissed or penalised for performing their task.
  - Has adequate resources to meet GDPR obligations.
- You can contract out the role of DPO externally.
- GDPR does not specify specific credentials for a DPO. However, they should have "professional experience and knowledge of data protection law" which is "proportionate to the type of processing your organisation carries out, taking into consideration the level of protection the data requires".
- The DPO should be aware of the responsibilities that the position entails.

ACTION PLAN – POLICIES AND PROCEDURES

- If you don't have one, write a data protection policy. If you do have one, review it.
- Consider amalgamating the data protection policy with your data/IT security policy if you have one. If you don't have one, write one!
  - Take this opportunity to review data security procedures and systems.
  - Look at where your data is stored and review access and security arrangements.
  - Make sure this assessment is extended to emails.
- Communicate the policy/policies to all staff and record that you have done so.
  - Ensure the policy/policies are drawn to the attention of relevant new employees.
- Empower your data protection officer to 'police' the policy.
  - Give him/her time, scope and authority to search out actual or potential breaches of the policy, to identify potential threats and to recommend corrective action.
- Decide on tools and procedures for handling objections and requests.
- Write policy statements for individuals and decide how and where to present them.
  - Review your standard email footer text.
- If you use email marketing, consider how you will move to 'opt in' and start implementation.

LEGITIMATE INTEREST ASSESSMENT

- The assessment template supplied on this course should meet the needs of most circumstances.
  - Digital (Microsoft Word and pdf) versions are available from CIM.
- An assessment should be completed for each group of data (ideally listing all the data within the group) and then filed. It should be periodically reviewed.
- ‘Best practice’ would be for the assessment to be carried out by someone with no involvement in the use of the data in order to reduce any possible conflict of interest.

A WORLD OF OPPORTUNITIES?

- Where can you help your clients?
- HIGH volume:
  - You can’t make money from just a few records.
- HIGH velocity:
  - The speed of managing data ties your customers in.
- HIGH variation:
  - The more variable the data the more important you are.
- HIGH value:
  - Make sure your customers are fully aware of the value you bring.

PERMISSION-BASED MARKETING

- Do you need a permission-based list?
  - Probably – under e-Privacy Regulation.
  - Possibly not under GDPR.
- Remember that e-Privacy Regulation applies only to electronic communication.

BUILDING A PERMISSION-BASED LIST

- You have to get permission!
- Think – “what’s in it for me?”.
- Be creative!
- Be honest. But don’t needlessly limit your options.
- Start now, using existing legislation and GDPR legitimate interest if you can.
- If you need to rely on ‘informed consent’ you need historic ‘GDPR standard’ evidence – if you don’t have it, you will need to ‘repermission’.
- There is going to be a new focus on ‘inbound’ marketing – website forms, social media, sales scripts – and more.
- Make use of ‘soft opt-in’ as far as possible.
- If they won’t consent – what have you really lost?