GDPR (EU General Data Protection Regulations) Implications for Small Businesses
If you store any data on any natural person (i.e. not a company acting as a virtual person), you are deemed by the law to be processing it, even if you never make use of it for any commercial purposes.

A few scary thoughts:
After May 25th, 2018, all the data you currently process on any natural person will no longer be legal. You must either delete, obfuscate or create a new legitimate basis on which to hold those data.

Non compliance with the DGPR carries heavy penalties of up to 4% of global turnover, or €20,000,000, **whichever is the greater**.

A legal precedent has been set in the UK for the value of distress caused to an individual through data leakage. An individual was awarded £2840 damages for such distress. Multiply that by the number of people on your mailing list and consider the consequences.

The Information Commissioners Office, responsible for dealing with complaints under GDPR and under current legislation has been made self-financing. All their government support is withdrawn and the only way they can raise funds is by levying fines. No business will be exempt from their search for revenue. The Commission's policy of pursuing businesses in the large, medium and small categories has already been declared.

Even though this is an EU law and we are leaving that club, the law locality relates to the end user. This means that even if your data is held in a non-European state, and a complaint is raised by a non-EU citizen, if they were in the EU at the time of entering the data concerned, the law applies.

What is Allowed
Under GDPR you must now prove that you have a legal basis for processing personally identifying data. The acceptable legal bases are:

- Consent
- Necessity for contract
- Legal obligation
- Protection of vital interest
- Public interest
- 'Legitimate interest'

Consent
Unlike most current practices where you tick a box to say that the organisation concerned can process your data, consent now has far more specific requirements before it can be recognised in law. Consent must be:

- Freely given (e.g. not in exchange for reward or competition entry)
- Explicit – you must tell them exactly what you are going to use the information for
- Demonstrable – you have to be able to prove that you never use it for other purposes

- Clearly distinguishable – data for different purposes must be held separately and identified as to its purpose
- Expressed in clear and plain language – no specialist terms or jargon, all phrases must be clear to anyone reading them
- Able to be withdrawn at any time
- As easy to withdraw as to grant
- Covered by parental consent under the age of 16 (currently 12 in the UK, thanks to Scotland, whose definition of a 'child' is anyone under the age of 12)

When seeking consent, you must provide the following information:

- Identity and contact details of person responsible for data management
- The legal organisation or entity that will process the data
- Details of the data recipients
- The length of and need for data storage
- The rights of the subject
- Details of how to withdraw their data
- Details of any automated decision making processes involved

Necessity for Contract

Where it is necessary to keep the data in order to fulfill your oblications under a contract. This is likely to be the best option under which to proceed with customers. The wording for 'consent' data processing is so open to interpretation that it is safer by far to make a contract with all your contacts. Whether this is in exchange for payment or not, is unimportant. What is important is that you word the contract carefully to make sure that there is no dispute over your use of the information.

Legal Obligation

The necessity of holding data on individuals for legal obligation covers areas such as holding of wills and other probate documentation. There is also a case for holding data for the purposes of warranties and other guarantees offered to customers for a fixed time. In the latter case, at the expiry of that period, the details must be erased. Also, where the warranty or guarantee information is used as the legal basis for processing data, communications in relation to that warranty are the only justifiable use of the data.

Protection of Vital Interest

This mainly covers data held for the purposes of health, where medical records need to be retained in the interest of the individual concerned.

Public Interest

The good old government get-out clause where they believe they can keep any information on anyone they like as long as they argue that it is in the public interest. The first few test cases will be watched with great interest. As for the rest of us in small to medium business, we can't really argue that selling a new widget just in time for the old one to wear out is in the public interest, so we can forget this one.

'Legitimate Interest'
This was included to keep data agents and behavioral marketeers from trafficking in the personal information of others. It simply states that the processing of those data should be 'in the interests of one organisation or of society as a whole'. On face value, it sounds like the ideal reason for a small business to keep personal information. However, digging a little deeper, you will find that this also involves gaining consent under all the new conditions, so is unlikely to be any more useful than just asking for consent again.

Actions Required from All Businesses

- Identify necessary data (What do we keep? Why? And how do we use it?)
- Determine the legal basis for keeping such data
- Decide on the most appropriate legal basis for future data processing
- Make that available before May 25th, whether it be a new consent process or contract based
- Erase all unnecessary data (that includes backups, redundant information and old paperwork that hasn't seen the light of day for years)
- Create a Data Protection Policy
- Create a Web Site Cookies Policy
- Create a new, more detailed Privacy Notice
- Define a policy for handling Access Requests
- Create a 'Right to be Forgotten' policy
- Create a complaints procedure
- Carry out risk assessments for all data repositories:
  - Web enquiries
  - E-Mails
  - Local computer records
  - Network computer records
  - Staff laptops
  - Mobile phones (business and personal)
  - Tablets and iPads
  - Removable and portable media
  - Paper records
  - Archives & backups
- Carry out adequate staff training to ensure compliance

What is in the Village Websmith's GDPR Package?

- Carry out a detailed risk assessment of all web-based data processing (web site enquiries and emails)
- Advise on the most appropriate legal basis for keeping records
- Advise on what data need to be kept, and which deleted in line with that basis
- Delete from web servers and all backups any data not being deemed necessary
- Review and amend all information on guestbook or testimonial pages to make sure of anonymity
- Create either consent request documentation or contract basis for keeping data
- Perform a 'purging' broadcast email to all contacts to ask them to join the new legal basis chosen
- Delete from current database and all backups, the information relating to anyone who requests removal
- Implement changes to enquiry forms and data harvesting to ensure compliance
- Provide the assurance of our own IASME/GDPR accreditation to cover those elements of your data held on our own servers
- Cover data on our web servers through our own professional indemnity insurance
- Write the web element of your data protection policy (I am happy to advise on in-house data management issues, but as I don't know your systems as well as our web servers, this can only be offered as an information adjunct)
- Create your web site cookies notice
- Create your web site privacy notice
- Create your Access Requests policy
- Create your Right to be Forgotten policy
- Create your complaints procedure
- Create new web pages for delivering policies and granting access plus 'right to be forgotten' requests – add to your existing Webinthebox® web site
- Offer remote advice on in-house data management (On site analysis and training of staff also available at cost)
- Analyse externally held data lists, e.g. MailChimp etc., and purge as per data held on our own servers. Plese note that we cannot be held responsible for purging externally held backup files. For that you will have to rely on the data manager
- Ensure that data management of your web site meets GDPR standards

Delivery should take 10-14 days. The legislation doesn't come into force until May 25th, 2018, but it is worth making the effort now, as closer to that date, when everyone else has woken up to the implications, all market places will be clogged with re-applications for consent, which will be very likely to slow down the process and deter many from responding to the huge number of requests that they will all undoubtedly receive.

Neil Hesman t/a The Village Websmith, Clear View, Main Road, Tintern, NP16 6SE, 01291 680187, admin@villagewebsmith.co.uk