Editorial

Journal editors and data: the General Data Protection Regulation (GDPR)

DOI: 10.20316/ESE.2018.44.18011

Please note that this article does not constitute legal advice, but presents a personal perspective, having investigated and implemented a GDPR policy for EASE. Readers should consult their organisation if they have any questions regarding implementation.

Few of you will have been able to ignore the large number of emails sent out at the end of May about the introduction of the General Data Protection Regulation (GDPR) passed by the European Parliament back in 2016 (https://gdpr-info.eu/). Hundreds of companies sent out a flurry of emails, responding to the apparent need to get affirmed consent to retain your records and communicate with you. No doubt you ignored several, answered others, and probably missed some (that may have gone into your spam box). The regulation has been introduced in an effort to protect the privacy of European citizens, and so applies not only to European organisations, but to anyone, anywhere, who holds and/or deals with data about European citizens.

The key requirements of relevance to journal editors are that any data is held for legal, legitimate, purposes, that consent has been given to hold the data, and that any individual - on request - may see what data on them you hold and require you to delete their information (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/). There are also requirements about data controllers, data managers, portability and several other details that are not included in this article since I am focusing on the direct implications for journal editors.

The tsunami of emails was spurred by the incorrect assumption that everyone needs to obtain renewed consent to both hold personal details and keep people on their email lists. In fact, many organisations do not need to ask for renewed consent, for example, EASE did not have to ask members for renewed permission. Not only did this misunderstanding add to the email overload, but it may result in problems for some organisations.

If you already have a contract or other formal agreement with an individual then you will need to retain certain information (eg names, addresses) in order to fulfil your obligations - for example providing copies of a journal to subscribers. Likewise, if you have an existing relationship with somebody (eg a reviewer) and their data are only used to continue the relationship (eg to ask them to review) then this constitutes a legitimate use of their data, and asking again for permission to hold their records is not required.

For the same reason, asking your community or members to affirm consent may cause problems if they do not answer because you have to interpret non-answers as negative - ie refusing you permission to hold data and communicate with them. Therefore you must think carefully before you ask for affirmation and be aware of the implications of anyone saying "no". For example, if a membership association asks for consent and several members do not reply then their details have to be removed. Deleting records would mean that the association could not provide member benefits, and so would be in breach of its obligations.

What does this mean for journal editors?

What data do you collect?

Any organisation, including the editorial office, must have a legitimate reason for collecting personal information about anyone. The most basic reason is for communication regarding your agreement with the individual as author, reviewer, subscriber, etc. However, it could be argued that additional demographic or personal data is also required (eg country, sex, etc) for legitimate reasons (eg to ensure diversity within your publication). If you feel you have a valid reason for collecting additional information you should discuss this within your organisation to obtain their agreement - and you may need to obtain consent from each individual for this additional information to be captured and retained.

Right to access

You should be able and willing to provide data on any individual if they ask for this - this means that you should be careful about any personal (ie unprofessional) comments made on individual records. Rating and ranking of individuals (eg reviewers) should be done in such a way that you would not be embarrassed to show them the records that you retain.

It is possible that an author may interpret this right of access to mean that they have the right to see all comments made about their article, including the "confidential comments for the editor". Since these confidential comments are made as part of a personal communication between the reviewer and the editor, and do not form part of the personal data held about an author, there should be no obligation for them to be made available to the authors.

Clear consent and the right to be forgotten

Most authors and reviewers self register on submission systems, so they have already provided consent for their information to be held. However, since editorial offices can add records without the individual's consent the large submission systems are introducing a one-time consent form so that when an author/reviewer signs on they are required to assert their permission for data to be held according to the journal's terms and conditions. Existing

users are only presented with this new consent form once, and if they do not consent then presumably the system does not let them log on, but reroutes them. If you are concerned, speak to your submission system vendor. You should also ensure that your submission system, or journal, has a clear Terms of Agreement page for individuals to read and check when they first register on the system - and it is important that this page should be clear and easy to understand.

You may have individuals (usually reviewers) who ask to be removed from the system - usually this is because they do not want any further invitations to review. In this case you have two options: you can "block" their record, or "anonymise" it. Ideally, it is better to block the record. This means that you retain your archive of who-reviewed-what but they will not be bothered with future invitations. In most systems it is not possible, or is hugely problematic, to totally delete records.

There are discussions about the rights of a reviewer or a rejected author to demand removal of their data. This would result in removal of all identifiable details so that the record is fully anonymised. However, losing the details about an individual could be problematic if an investigation of any submission is needed in the future (eg accusations of fraud or misconduct). There is also the question of whether removing data would interfere with your "core business", in which case this reason may provide exception to the individual's right to be forgotten. Therefore, such arguments for the legitimate need to retain details are persuasive. If you receive a request for the record to be deleted or fully anonymised you should discuss the situation within your organisation.

What do you do with personal data?

Probably the most important feature of the GDPR is to remind everyone to show respect for personal data and ensure that it is not misused. Fortunately, within our environment misuse of data is relatively small. However, this regulation does emphasise the need for treating any personal data with respect and always considering it confidential information, only to be shared as agreed by industry norms, eg author names and affiliation with reviewers (assuming single-blind or open review), and subscriber names and addresses with the printers, etc.

Confidentiality is a growing issue in the social world (hence the GDPR ruling), and editorial teams are encouraged to remind everyone about their duty to treat all submissions with care. I was recently told of an editorial administrator who realised that an author was a friend of a friend, so he approached her on Facebook. The author felt that this breached her confidential relationship with the journal. For similar reasons, reviewers should be reminded of their obligation to treat all invitations to review as confidential agreements between them and the journal editors and not to disclose information about the authors or the article before publication without explicit agreement from both the editors and the author(s) (for example, see the ICMJE guidelines: http://www.icmje.org/recommendations/browse/roles-and-responsibilities/responsibilities-in-the-submission-and-peer-peview-process.html).

It is common to list reviewers in the journal at the end of the year to thank them. Would this constitute a breach of confidentiality, and something for which confirmation of permission is required? This is probably an area where industry practice and existing norms should take precedence. It is unlikely that reviewers have been asked to affirm consent to being listed, but they gain some benefit from being named and thanked. In this case the benefit to the reviewers would mean that the practice should continue, and that formal assent need not be requested. Also bear in mind that if formal assent is sought it would mean that those who did not reply would be omitted for the list.

Terms and conditions and standard email templates

The GDPR implementation should be treated as an opportunity to review the agreements with your editors, authors, subscribers and reviewers. It should also make you check the standard email and registration templates in use. Are you clear about how you hold data on individuals, and what you do (and just as importantly, what you do not do) with their data? This could be an opportunity to demonstrate that you are being honest and ethical with personal data. Are your standard email templates clear about what rights and responsibilities both the individuals and the editors and publishers promise to uphold? It may be time to revise and clarify them.

Final words

Whilst the implementation of GDPR has been met with cynicism and irritation, feeling that it won't reduce the level of spamming and will only introduce an additional level of administration for honest companies, it should not be overly onerous for journal editors, and may even be an opportunity.

Resources and further reading

There has been a great deal written about the GDPR and its potential impact on different companies. Below are two general resources which may be used as guidelines:

GDPR information (unofficial) Portal:
https://www.eugdpr.org/

UK Information Commission Office official guidance:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Pippa Smart
PSP Consulting and EASE President
pippa.smart@gmail.com
http://orcid.org/0000-0002-5528-4704