

“ Further to the information we provided on the GDPR in previous MU communications, we have put together some practical examples of how the GDPR may impact on MU members. Set out below are three case studies, the gigging musician, the music teacher and the crowd funded musician. These cover the basic issues around collecting email addresses, marketing, sharing information, registration, sharing exam results and working with pupil data. ”

*Dawn Rodger
MU In-House Solicitor*

1 The Gigging Musician

Alan is a gigging musician who plays regularly at a local venue.

At the venue a noticeboard has pinned to it a paper “sign-up form” where fans can add their names and e-mail addresses. Alan uses those names and addresses to notify fans about upcoming gigs, tours and updates to his online blog.

Alan also tours occasionally. During the tours he usually sets up a merchandising stall/stand outside each gig. He uses an iPad and/or a PC to collect information from fans including their name, address, mobile number and e-mail address.

Alan uses this information in the same way that he uses the noticeboard information from his local gigs, but in addition he shares the electronic information with other bands, with promoters on the festival circuit and with his record label.

Alan has a blog and a website. The website has a “cookie” warning and an old fashioned “opt-out” consent form, but no GDPR privacy notice.

Alan has a database of some 1,000 names and e-mail addresses gathered over the years by a combination of the methods mentioned above.

Frequently Asked Questions

A What can Alan do with his old database of names and e-mail addresses? Will the “soft opt-in” help?

Answer:

New consents will generally be required for email/SMS marketing. Direct Mail (i.e. post) has less strict requirements. But all email and text-message marketing requires consent on a transparent, informed and “granular” basis.

That means separate opt-ins for each type of contact Alan wants to make e.g. a tick box for email and another box for SMS.

Alan should NOT use “opt-outs” or pre-ticked boxes.

The soft opt-in only applies if Alan has sold products or services (or negotiated with a view to sale) to people he is contacting, and they opted in at the outset, and have been given a chance to opt out whenever they have been contacted since.

Given that Alan has collected information just for marketing purposes (i.e. not in connection with any sale) the soft opt-in is unlikely to help him.

The ICO publishes a very helpful CHECKLIST about direct marketing for small businesses.

B Can he continue to collect data via the noticeboard and/or the merchandising stand?

Answer:

Yes. But it is personal data so he will need consent to market to fans.

Paper records can still be subject to GDPR.

But Alan probably transfers the noticeboard information onto a computer for emailing purposes anyway – once it's on there, GDPR will apply.

C What consents will he need?

Answer:

See above. Also:

Pre-ticked opt-in boxes are banned under the GDPR.

Alan cannot rely on silence, inactivity, default settings, or “general” terms and conditions.

GDPR does not specifically ban opt-out boxes but they are essentially the same as pre-ticked boxes and so unlikely to comply.

Consent under the GDPR must be a positive indication and must be separate from other matters i.e. Alan should not include it in the middle of other terms and conditions.

Remember to make the opt-ins “granular”. Be clear in the consent form about what the data will be used for.

Use a Privacy Notice.

D With whom can he share the data he collects?

Answer:

Fans need to be told about any plans to share the data.

It will not be enough to identify potential recipients as a generally-defined class of persons.

So if Alan wants to share information with a local band which plays at the same venue, he should say so – and identify that band.

Likewise “festival promoters” cannot be used to describe the class of persons to whom the date will be sent. A name (and possibly other identifying material) will be needed.

E What Privacy notices or other documentation will he need?

Answer:

It makes sense to link a Privacy Notice from any sign-up form or any website or blog.

Alan should have a Privacy Standard too (sometimes called a privacy or GDPR compliance policy).

Consents need to be separate documents – so they must not be embedded in a general set of terms and conditions or “hidden away” in fine print.

F What rights might fans have in relation in the data Alan holds about them?

Answer:

Fans can make a Subject Access Request to get access to the data Alan holds about them.

As a rule Alan can't charge a fee for replying and should reply ASAP and in any event inside a month.

They can also ask Alan to delete their data. They can withdraw consent. They can ask for the data to be corrected. There are other rights, too.

2 The Music Teacher

Carole teaches music to children between the ages of 7 and 18.

She has a contract with two local schools to teach on site at the schools and at her home and at the homes of pupils.

Both contracts require her to invoice parents directly for the work done.

Carole maintains a database of pupils on her PC. It includes past and present pupils and a “prospects” list for pupils to whom she intends to try to provide services in the future.

Carole’s database includes the name and address of each child, parental details and bank details for invoicing purposes. In addition, details about each pupil’s examination history are recorded, and a “notes” section details Carole’s opinions and thoughts in relation to each pupil.

Carole supplies a monthly list of pupils to each of the two schools she works with and provides quarterly reports to all the parents she has contracts with. The reports are cc’d to each school.

Carole publishes the exam results in a regular newsletter, which is copied to each school. Carole is not registered with the ICO.

Frequently Asked Questions

A Is Carole processing personal data? Does GDPR apply to her?

Answer:

Yes. She has an automated (i.e. computer) database and the information she keeps identifies natural (i.e. real) persons.

Bear in mind that the “Notes” section is going to be caught as data under GDPR since “expressions of opinion” are specifically included as items of personal data.

Also data that on its own might not identify a person but, taken together with some other data, shows identity, is personal data under GDPR.

Carole “processes” data simply by storing it on her PC. She processes it when she adds to the exam results or “Notes” sections, or runs billing software that takes names and bank details etc from her database.

B What registration steps must Carole take?

Answer:

Technically registration with the ICO is no longer necessary under GDPR. But a fee may be payable.

C Does Carole have to pay a fee to the ICO?

Answer:

In short, most small business will need to pay a fee of £40 per annum.

There are some exemptions but they are likely to be of limited application in practice. If Carole only had billing information (e.g. parent’s name and address) an exemption might apply – but Carole’s information goes well beyond that.

If all the processing is done on paper i.e. with no computer, another exemption applies. But the administrative burden of doing everything on paper is likely going to outweigh the cost of the fee, for most teachers.

The ICO has a useful guidance note about the new fee regime.

D What consents does Carole need?

Answer:

Carole probably does not need consent to process data about her existing pupils – but if she wants to get it anyway, then for under-13s, parental consent is required.

GDPR allows Carole to process personal data for the purposes of a contract she is performing. The data she uses is very much of that sort. So consent is neither necessary nor indeed the best way to comply.

In many cases personal data will be processed for the purposes of a contract. It is likely that e.g. provision of music tuition will always involve some underlying express (or implied) contract to provide services.

One of the legitimate bases for processing data relates specifically to the performance of a contract.

The ICO's website puts it like this: you can process someone's personal data "if you need to do so to fulfil your contractual obligations to them".

Carole's actions are probably necessary for her to perform her part of her contract. How else can she invoice parents or keep track of pupil progress? (Note that processing must be "necessary" here – but in Carole's case that seems likely.)

Consent therefore is probably strictly not required and good practice suggests that Carole ought not to rely on consent if she has another basis to process data.

Carole should however document what she's doing and why she's doing it – so she can show she has applied herself to the point.

For former pupils or prospects, however, she is probably going to be engaged in direct marketing and should get consent as described in Case Study 1.

E Can Carole continue to keep all of the information she stores at present?

Answer::

Yes, provided she thinks about the consent issue mentioned above. She is not storing superfluous material. Limiting the data she keeps is a principle of lawful processing.

She needs to think about whether she ever stores Special Category ("Sensitive") Personal data – which includes details about health, sexuality, religion, Trade Union membership etc.

It might be that Carole records health-related information in her "Notes" data e.g. to help her deal with a pupil with a disability. She will need explicit consent to store that information – even if she is otherwise lawfully processing data to perform a contract.

F Can Carole copy the schools in to her newsletters?

Answer:

Almost certainly – she has a contract with the schools, too, and the newsletters form part of her performance of the contract. See also the next question about exam results.

But it would be good practice to tell pupils that this is intended. Being transparent about processing data is a key principle (and new under GDPR).

G Can Carole publish information about exam results?

Answer:

Yes. The results can even be published in e.g. the local newspaper.

But Carole should be alive to any complaints or objections she receives – and if a parent asks Carole to avoid publishing data for a given child, good practice (not to mention customer service!) might suggest that such a request should be granted.

It is also good practice to ensure that parents and pupils are told in advance what publications are planned. Carole's newsletter might include information about this; or her terms of business or introductory letter could set out what she usually does to publish results.

The ICO has some useful Guidance on this subject.

H Can Carole publish photographic information?

Answer:

Photographs that identify people can be personal data for GDPR purposes.

Photos taken for personal use are not caught by GDPR.

But if Carole wants to use a photo of a pupil e.g. in her newsletter, or in a "brochure" selling her services, it makes good compliance sense (and good business sense) to get consent up front. The consent should be clear, transparent, opt-in only and specific e.g. "I consent to my/my son's photograph being used in the July edition of Carole's newsletter and in Carole's 2018/19 "piano lessons" brochure".

3 The Crowd-funded Musician

Mo wants to record and release a digital album.

Mo signs up to “pledgemusic.com” a crowdfunding website that will enable him to raise money for the album.

Mo intends to provide a digital-only copy of his album to the subscribers to the pledgemusic.com crowdfunding drive.

Mo will download a list of subscribers from pledgemusic.com to enable him to fulfil orders for the digital album when it is ready.

Mo will also add the subscribers to the database he keeps on his computer. He will use that to market details of his next crowdfunding venture and to provide details of his subscribers to other crowdfunders that he thinks they might be interested in.

Mo has an old DPA 98 – compatible consent for his existing subscribers but has not updated that to deal with GDPR.

Frequently Asked Questions

A Must Mo register with the ICO/pay a £40.00 fee?

Answer:

Registration is unnecessary but a fee is payable by most small businesses.

If the only information Mo keeps is contact details to enable him to deliver his goods and advertise his new ones (i.e. digital albums) then arguably one of the exemptions applies. The law is brand new and less than 100% clear. If in doubt it might be worthwhile Mo contacting the ICO directly to ask if he is exempt.

B What consents does Mo need?

Answer:

Mo may not need consent at all to fulfil his album orders. He has to process data to perform the contract he is making with each person who orders the album – see also Case Study 2 about contractual performance.

He should document his decision – what he’s doing, in GDPR terms, and why.

For direct marketing see below.

C Can Mo use his old consent in the post-GDPR world?

Answer:

The “soft opt-in” may apply – see Case Study 1.

But the easiest approach is probably to get subscribers to renew with GDPR-compliant consent – also covered, in the first 2 Case Studies. Remember consent needs to be specific, informed and granular.

D Can Mo continue to use the information he collects for the purposes described above?

Answer:

Yes, in so far as he is marketing his own products to his own customers.

But old consents will probably not enable him to give details of his subscribers to third parties. Mo will need new consents in which he expressly identifies the third parties (e.g. other crowdfunding artists) to whom he intends to release the subscribers’ details.

See the other Case Studies for more information about identifying third parties.

Short Glossary

Personal Data: any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

Special Category/Sensitive Personal Data: information about race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation.

Processing: any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, alteration, retrieval, use, disclosure by transmission, dissemination or otherwise making available, combination, erasure or destruction.

Granular Consent: consent given specifically and separately (e.g. by a set of different tick-boxes – one for SMS, one for email etc) for different types of contact for e.g. marketing purposes.

Soft Opt-In: a limited exemption permitting reliance on an old consent provided by former customers; will not apply in lots of cases.

DISCLAIMER

These FAQs are provided for general information only and are not a substitute for specific legal/compliance advice. Everyone's circumstances are different and only case-specific advice is generally reliable. The MU cannot offer individual compliance advice or templates to members in relation to GDPR.