

Forum:[Hack Forums](#)

Thread: [GDPR Discussion](#)

Omniscient - June 24, 2018, 8:01 pm

This is direct quote from the GDPR law.

Quote:However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

This is in a nutshell why we're not going to just delete accounts. We have a legal obligation to retain data. There is also archival purpose and freedom of expression.

I'm getting contacts requesting accounts deletions. We are not going to do it and under GDPR we have exemptions that directly apply to our community.

There might be some situations though where accounts might get altered or posts edited/deleted. We've always been against the posting of private data but there have been threads where members were asked to post their social media accounts or emails in contests and giveaways. Those may get deleted if requested. We don't agree with situations where members exposed their private information on the forum but now GDPR makes it a legal issue.

We are going to be as compliant as possible, if not fully compliant. We're almost done with the export feature.

I thank everyone who is bearing with us at this time and if you have questions or concerns I'm happy to try and discuss the situation. It's a complex law and we're a complex site. Unfortunately this is so new that many sites haven't done anything to be compliant and there aren't many sites like HF which we can draw examples from. I do hope that HF is the site that sets the example and we're working hard to make that happen.

Thank you.

btw, if you wish to read the GDPR yourself then go for it:

<https://gdpr-info.eu/>

Charger - June 24, 2018, 9:39 pm

GDPR seems really stupid. Seems like the EU is trying to change the internet (but failing) like the US did with the creation of the DMCA.

BeNT- - June 24, 2018, 9:48 pm

Wow, that is a shit ton of Legalese in a paragraph.

No wonder Omni's bald.

Fuck. Cheers. B.

Truth - June 25, 2018, 1:39 am

Such BS law, I know another forum deciding to just shut down because of it.

Anyways, Thank you Omni for doing what it takes to keep this forum alive. I can't even imagine the headaches you had over the years.

Fire - June 25, 2018, 2:38 am

(Jun 24, 2018 09:39 PM)Charger Wrote: [\[CITE\]](#) GDPR seems really stupid. Seems like the EU is trying to change the internet (but failing) like the US did with the creation of the DMCA.

It seems stupid because you are talking out of your ass. Go ahead and read before posting bullshit.

Kraith - June 25, 2018, 11:39 am

So question what if someone just edits their post to "null" or "Delete"? Then they don't have to even worry about asking someone to delete material they didn't want posted

Krueger - June 25, 2018, 12:57 pm

(Jun 24, 2018 09:48 PM)BeNT- Wrote: [\[CITE\]](#) Wow, that is a shit ton of Legalese in a paragraph.

No wonder Omni's bald.

Fuck. Cheers. B.

This ones good jokes..

I feel you Omni youll get trough it no worries youve been the greatest mind i came accross on deh webs and hf i support you man

Secret Agent - June 25, 2018, 2:31 pm

Quote:You consent that data we have stored on your account may be downloaded only once per 30 day period. This will provide you the most accurate results of what we have stored. Data exports manually done more than once per 30 days will incur a \$10 fee for processing.

Do we just PM Omni requesting a download of our account data?

PoPHF - June 25, 2018, 2:34 pm

(Jun 25, 2018 02:31 PM)Secret Agent Wrote: [\[CITE\]](#) Do we just PM Omni requesting a download of our account data?

User CP

Should be a tab at the bottom of the list on the left

Kraith - June 25, 2018, 9:51 pm

(Jun 25, 2018 02:34 PM)PoPHF Wrote: [\[CITE\]](#) User CP

Should be a tab at the bottom of the list on the left

Not functional at the current moment in time.

Warbiest - June 26, 2018, 12:41 am

(Jun 25, 2018 09:51 PM)Kraith Wrote: [\[CITE\]](#) Not functional at the current moment in time.

It's new so there might be issues, but it does work.

Omni announced it should be functional now and I already successfully tested it.

Fortunate - June 26, 2018, 12:57 am

(Jun 25, 2018 01:39 AM)TryAgain Wrote: [\[CITE\]](#) Such BS law, I know another forum deciding to just shut down because of it.

Anyways, Thank you Omni for doing what it takes to keep this forum alive. I can't even imagine the

headaches you had over the years.

Such a shitty forum then. It's a pain in the ass for the website, but good for you.

The forum owners were lazy assholes or had something to hide.

Vegas - June 26, 2018, 5:05 am

I'm not going to lie, this tickles my titties, fellas.

Michael - June 26, 2018, 5:15 am

A lot of people want to have their say about this, but barely have an idea about what this really is about, so I'll just leave this here:

Spoiler [\(Click to View\)](#)

And for HF, Omniscient is doing a good job imo. You're really trying your best to comply. Most users won't like this, but in the end, it's better for all of us.

Vegas - June 26, 2018, 5:45 am

Sheeeeeiiit. All the reputation ratings lost. How will I refer people to my many great totally important accolades >:C

overlude - June 26, 2018, 4:16 pm

A few queries, Omniscient.

(btw, can't use full text editor so formatting my may suck, sorry if it makes this harder to read, error: Fatal error: Cannot redeclare custom_permission_check() in /home/hfaccount/domains/hackforums.net/public_html/inc/functions_custom.php on line 150)

First query:

Using your quote from the GDPR, you said: "This is in a nutshell why we're not going to just delete accounts. We have a legal obligation to retain data. There is also archival purpose and freedom of expression."

Which part of that quote are you using as justification? For archival purposes, you'd retain a right to keep posts (which you did anyway), but for other information stored (email addresses, IPs, names, addresses from payment details) the freedom of expression doesn't apply. Your quote lists all the valid reasons for processing data (beyond consent), which one is being used to continue processing this personal data (without consent)?

For clarification, you can say retaining IPs (of banned users) under the "legitimate business interests" clause is valid to enforce your one account policy. I'm just clarifying which reason for processing is used for email addresses and billing information.

Second set of queries stem from your privacy policy:

(hackforums.net/misc.php?action=help&hid=12) (presuming this is still the active privacy policy). -- (I cannot link to this policy, possible to allow inter-site linking for users with < 50 posts?)

1. Do you still store billing data (names, addresses) from when you processed PayPal payments, or still request this info for Bitcoin payments? It isn't mentioned there, hence I ask.

2. From your policy: "Anyone reversing payments to HF are subject to a closed account and their payment details and account information placed directly into their signature for public viewing. If you want to reverse a payment to HF then go for it but we will make sure you are named and shamed and the data will not be removed. Your payment and account details will be made public and searchable at Google. You are warned."

I'm not particularly active here (as you can tell) so I don't know if you use this name and shame policy much. This is certainly a violation of the GDPR and, in general, a bit concerning from a privacy perspective. Chargebacks suck, but this is a very dangerous policy, and often those charging back may not be using their own personal details, so the details of some person have been leaked to a community notorious for various illegal acts to persons.

Do you plan to wipe all this stuff from your privacy policy and create a GDPR compliant privacy policy in its place? Additionally, do you plan to (optionally) offer these same GDPR rights to all users across the world, not just those resident in the EU (as a show of your dedication to protecting users' privacy).

This site's members have been known to be toxic towards each other in the past, specifically by doxing, swatting, etc. Of course, I don't suggest you support any of these actions, but naturally your site (as the largest hacking forum) attracts these types. Due to this, I hope you'll try your best to always ensure the highest standards of privacy. You can't babysit users, but you can hopefully set an example by showing a great level of respect for individual user privacy (as I'm sure you already do).

Thanks!

Omniscient - June 26, 2018, 4:40 pm

Quote:I'm just clarifying which reason for processing is used for email addresses and billing information.

We don't process billing information since moving to cryptos. Anyone can do an export to see their PII we have. It's very minimal.

Quote:Second set of queries stem from your privacy policy:
The privacy policy has to be rewritten still. Realize this is a LOT of work and indeed it's constantly changing as we realize new things and how they apply to HF.

Quote:1. Do you still store billing data (names, addresses) from when you processed PayPal payments, or still request this info for Bitcoin payments? It isn't mentioned there, hence I ask.
Yes, that data we have currently saved in archive format but is not part of the HF database. I think under GDPR that type of data doesn't necessarily have to be deleted if there is a legitimate purpose in keeping it, which we have. Note that before GDPR it was standard practice to just save data constantly, persistently, and forever. Now of course adjustments have to be made for compliance to GDPR.

Quote:I'm not particularly active here (as you can tell) so I don't know if you use this name and shame policy much.
No longer needed or used since we moved to crypto. But I'm not so sure it's against GDPR to have it anyways since it's a legal issue where I have been scammed. In any case, we no longer even require valid billing address in payments. With cryptos we process payments very differently and even more securely and privately for members with no risk to either party.

Quote:Do you plan to wipe all this stuff from your privacy policy and create a GDPR compliant privacy policy in its place?

Yes, I plan on rewriting policy to be GDPR compliant.

Quote:do you plan to (optionally) offer these same GDPR rights to all users across the world, not just those resident in the EU (as a show of your dedication to protecting users' privacy).

I intend to make one policy but some protections and options that the GDPR requires of me may not be applied to non-EU citizens.

Note that basically anyone making very serious requirements of me because of GDPR I will require them to prove their identity to me and EU citizenship. This the GDPR allows. So if you're not willing to send me your passport or national identification card you can forget even asking for GDPR protections.

Quote:Due to this, I hope you'll try your best to always ensure the highest standards of privacy.

It's always been a policy on HF that you were not suppose to post private member data. Exception was Deal Disputes in screenshot format only. Even that I believe is GDPR compliant consider the legal nature and public interest in knowing who a scammer is.

Overall members shouldn't worry about HF and what we do with your info. Because really we do nothing with it. It's useful to catch scammers and ban evaders and provide site safety for members. If you're a criminal and want your history erased to remove evidence then you shouldn't be asking for protections from a law, that would be ironic.

Black Hat - June 26, 2018, 4:51 pm

(Jun 26, 2018 04:40 PM)Omniscient Wrote: [\[CITE\]](#) We don't process billing information since moving to cryptos. Anyone can do an export to see their PII we have. It's very minimal.

The privacy policy has to be rewritten still. Realize this is a LOT of work and indeed it's constantly changing as we realize new things and how they apply to HF.

Yes, that data we have currently saved in archive format but is not part of the HF database. I think under GDRP that type of data doesn't necessarily have to be deleted if there is a legitimate purpose in keeping it, which we have. Note that before GDPR it was standard practice to just save data constantly, persistently, and forever. Now of course adjustments have to be made for compliance to GDPR.

No longer needed or used since we moved to crypto. But I'm not so sure it's against GDPR to have it anyways since it's a legal issue where I have been scammed. In any case, we no longer even require valid billing address in payments. With cryptos we process payments very differently and even more securely and privately for members with no risk to either party.

Yes, I plan on rewriting policy to be GDPR compliant.

I intend to make one policy but some protections and options that the GDPR requires of me may not be applied to non-EU citizens.

Note that basically anyone making very serious requirements of me because of GDPR I will require

them to prove their identity to me and EU citizenship. This the GDPR allows. So if you're not willing to send me your passport or national identification card you can forget even asking for GDPR protections.

It's always been a policy on HF that you were not suppose to post private member data. Exception was Deal Disputes in screenshot format only. Even that I believe is GDPR compliant consider the legal nature and public interest in knowing who a scammer is.

Overall members shouldn't worry about HF and what we do with your info. Because really we do nothing with it. It's useful to catch scammers and ban evaders and provide site safety for members. If you're a criminal and want your history erased to remove evidence then you shouldn't be asking for protections from a law, that would be ironic.

Just curious as to what the possible implications for HF could be if you weren't operating in compliance with the GDPR? I'm guessing HF would be blacklisted by EU internet service providers, payment/data processors or something along these lines?

Omniscient - June 26, 2018, 5:09 pm

Quote:Just curious as to what the possible implications for HF could be if you weren't operating in compliance with the GDPR?

Good question. One that I have no answer for.

Silver Fang - June 26, 2018, 5:22 pm

(Jun 24, 2018 09:39 PM)Charger Wrote: [\[CITE\]](#) GDPR seems really stupid. Seems like the EU is trying to change the internet (but failing) like the US did with the creation of the DMCA.

Why exactly is GDPR stupid/failing?

Isn't it good for the users to know what information they are gathering about them?

Omniscient - June 26, 2018, 5:27 pm

Quote:Isn't it good for the users to know what information they are gathering about them

Yes, and it's good to know how it's used. Unsure though if it's good to be deleted if you already approved of the processing. The GDPR gives people a few rights which are way beyond normal.

Silver Fang - June 26, 2018, 5:40 pm

(Jun 26, 2018 05:27 PM)Omniscient Wrote: [\[CITE\]](#) Yes, and it's good to know how it's used. Unsure though if it's good to be deleted if you already approved of the processing. The GDPR gives people a few rights which are way beyond normal.

Well 'normal' isn't always the correct path or choice.

Change could be better, in my mind i don't see any setback from my perspective as a user.

Omniscient - June 26, 2018, 5:46 pm

Quote:in my mind i don't see any setback from my perspective as a user

Exactly why this law sucks. Written by end-users who don't run internet sites. The full-burden of this law is entirely on website operators and realistically well beyond that. Any places that holds PII are under this law that includes places like hospitals or your local electric company not just websites. GDPR is about the processing of personal data.

So let's say you're a hospital in the USA. You have an EU citizen visiting America and while here gets injured or sick. When you go to a hospital they begin to get your data. They now fall under the GDPR. When an EU citizen now travels any hotel or resort they stay at falls under GDPR. Do you realize the burden that is for business who are not in EU? Heck, I'm sure EU businesses feel like this is a burden too.

So yeah, from user perspective it's no big deal. But are you unable to see the other side?

Just read this:

<https://hospitalitytech.com/hospitality-unprepared-gdpr>

overlude - June 26, 2018, 5:51 pm

(Jun 26, 2018 05:27 PM)Omniscient Wrote: [\[CITE\]](#) Yes, and it's good to know how it's used. Unsure though if it's good to be deleted if you already approved of the processing. The GDPR gives people a few rights which are way beyond normal.

I think it gives necessary rights. People should retain control over the processing of their data to the extent it is necessary. The previous data protection legislation (in the EU) is from 1998, clearly a lot has changed since then, notably our digital footprint on the Internet. I don't think it gives rights beyond the ordinary or is detrimental to businesses. There are methods of consent to allow you to use data reasonably even if the subject doesn't want you to, where they couldn't reasonably expect the processing of their data. e.g. the right to erasure is really just a right to withdraw consent, data processed under other reasons can still be processed. Of course, a business can make wild interpretations of the GDPR to give it a broad range of rights but (if reported) it won't hold.

I suppose you'll just have to interpret the act as best you can and apply it in your way. I probably don't agree with some of the things in your reply to me, but whether they're violations of the GDPR is anyone's guess, it's not exactly written perfectly in a way that you can be confident you're applying it right. Perhaps worth seeing a lawyer/consultancy firm regardless if you intend to keep data like addresses (I would at least), but emails and IPs are somewhat trivial.

Silver Fang - June 26, 2018, 5:58 pm

(Jun 26, 2018 05:46 PM)Omniscient Wrote: [\[CITE\]](#) Exactly why this law sucks. Written by end-users who don't run internet sites. The full-burden of this law is entirely on website operators and realistically well beyond that. Any places that holds PII are under this law that includes places like hospitals or your local electric company not just websites. GDPR is about the processing of personal data.

But as a user wouldn't you ensure that your private information are stored secured and to know the details of what they are gathering about you?

Also the quality of the cyber security will increase overall which is also really good for new developers in the future so they can grow with this.

When companies are GDPR compliant they will be able to operate with entire EU without worrying about laws.

As a user you can feel safer with the GDPR implementation at least from a personal perspective.

As a developer i see the hard work that has to be done.

The one thing that worries me is that if people can't choose to stay anonymous in the future, what i mean by this is the principle about taking microsteps into wrong direction as many countries have and it has affected the net neutrality along with the right of being anonymous.

As people will more and more decide to walk away from sites that are not GDPR compliant, this is included with all the other microsteps such as ISPS being threatened by governments to send out Data and IP belongings.

There should be laws to prohibit from overstepping where it actually causes damage for the 'free internet'

(Jun 26, 2018 05:46 PM)Omniscient Wrote: [\[CITE\]](#) So let's say you're a hospital in the USA. You have an EU citizen visiting America and while here gets injured or sick. When you go to a hospital they begin to get your data. They now fall under the GDPR. When an EU citizen now travels any

hotel or resort they stay at falls under GDPR. Do you realize the burden that is for business who are not in EU? Heck, I'm sure EU businesses feel like this is a burden too.

I see the work that has to be made, but could it be for the better? I believe so.

Exactly as we have laws today, they were made at some point and were considered to be bad or risky or alike but further in the time we understood it was needed.

About your example, I didn't know US companies have to change also. I thought this was forced to within EU to begin with..

Are you forced to use GDPR or to offer it if you are an US company at this time?

Omniscient - June 26, 2018, 6:18 pm

Quote: People should retain control over the processing of their data to the extent it is necessary.

You have full control by not joining. I stopped using my Facebook accounts a very long time ago. I am careful about sites I join and if I am worried about abuse of the information I give them then I don't join.

Quote: I don't think it gives rights beyond the ordinary or is detrimental to businesses
I assume you don't own a business or at least one that has to comply with GDPR.

Quote: There are methods of consent to allow you to use data reasonably even if the subject doesn't want you to

There is a number of things written into GDPR which requires a lot of work on the part of businesses. Just trying to understand the full scope of this huge law and how it applies to your business is a vast undertaking. I am easily 50+ hours into my own research and implementation trying to be compliant. And I bet another 20-50 hours gets logged before this is done. I'm one small site, so imagine your a multinational corporation with thousands of employees. They not only have to comply but if they don't they do risk facing the \$20 million fine for each violation.

Quote: I suppose you'll just have to interpret the act as best you can and apply it in your way.

I am listening to feedback and doing my absolute best to quote the actual law when I do interpret. I don't want to quote articles about the law or posts from the web. I prefer to read the law myself and use the words in it to justify my own policy. That's the only way imho we can be compliant.

The current agreement will likely be changed and updated and definitely the Help Doc will get completely rewritten too. Oh, we'll also be adding that little cookie popup thing soon too. More annoying crap.

Quote: Perhaps worth seeing a lawyer/consultancy firm regardless if you intend to keep data like addresses

I probably have read more about this law than a US lawyer. Also, I don't intend to keep addresses. I may have to go into some archive folders and just delete all my very old backups. I still have site files from 10 years ago, which I'm willing to bet most webmasters do that. You run backups, drop into folder, and forget it. No one puts an expiration date on files to self-delete.

Quote: But as a user wouldn't you ensure that your private information are stored secured and to know the details of what they are gathering about you?

100% agreed that this is a good thing. I love the data portability part of the law.

Quote: Also the quality of the cyber security will increase overall which is also really good for new developers in the future so they can grow with this.

I don't think that's true we'll see an increase in better security. If anything because GDPR requires that any data breaches get reported within 72 hours I think we'll hear more about breaches which previously might not have been reported at all. I'm sure sites are penetrated all the time and no one

is informed. Sometimes it was a whistleblower who told everyone or even the hackers.

Quote: The one thing that worries me is that if people can't choose to stay anonymous in the future That doesn't bother me too much because HF has always wanted members to maintain their privacy as best as possible.

Kraith - June 26, 2018, 6:25 pm

Omni, I don't understand how a European law is messing with your site. I understand that there are many EU users on the site. But why does it apply to a site you run out of the US? Since when do other country's laws even effect us? I know pirating sites that constantly get cease and desists that aren't affected because they aren't hosted in America.. Shouldn't the same idea be present here, considering the site isn't run or hosted within that country so the only laws that apply should be native?

Silver Fang - June 26, 2018, 6:47 pm

(Jun 26, 2018 06:18 PM)Omniscient Wrote: [CITE](#) I don't think that's true we'll see an increase in better security. If anything because GDPR requires that any data breaches get reported within 72 hours I think we'll hear more about breaches which previously might not have been reported at all. I'm sure sites are penetrated all the time and no one is informed. Sometimes it was a whistleblower who told everyone or even the hackers.

You haven't taken into account that developers will have easier to receives big fines if they don't protect the data according to standards and if they don't report it?

By the nature developers will prioritize the data safety especially the userdata due to this law and by that the quality of security will improve in a sense of smaller business sites for example.

add: About who's notifying about the breaches in the first places of course comes probably later, however i do think people will be more efficient with security updates.

This law in a sense will force people to maintain the user data much more safer and by nature by knowing the fee's or penalty for not protecting the data that is within the sense of law will be there to keep everyone in line.

After all, as a user my personal information should be considered a privilege to have and with that comes the responsibility to have it. Ethic and morals have maintained my personal details before now i know the law will also step up as a reminder of it.

I believe there will updates with this law in the future though!

Note: Is i said i am worried about how GDPR will be used in the future, if it will "help" companies to force people to leave their details to use important services that people need.

Also i am worried that companies will want more information about personal details so that they can "Believe the data to be GDPR eligible", or else they wont protect it or alike.

I agree with the hard work that has to be done and the cost overall that could come with it for that i would like to thank everyone who goes with the GDPR law.

Enronitis - June 26, 2018, 6:57 pm

I have been working with my employer to figure all of this out as it screws with a number of our international businesses, and as stated, it's a shit show to say the least.

We have a law-firm working full time on bringing us fully up to date.

@Omniscient, I'd be happy to discuss some of this with you, and even pass any specific queries you have to our retained firm.

Regardless, whether it ends up being good for the end user or not, its certainly screwing a lot of

businesses and as mentioned, almost no one is technically fully "compliant" with many opting to jump ship completely.

Gotta love the law sometimes ?

Silver Fang - June 26, 2018, 7:08 pm

(Jun 26, 2018 06:25 PM)Kraith Wrote: [\[CITE\]](#) Omni, I don't understand how a European law is messing with your site. I understand that there are many EU users on the site. But why does it apply to a site you run out of the US? Since when do other country's laws even effect us? I know pirating sites that constantly get cease and desists that aren't affected because they aren't hosted in America.. Shouldn't the same idea be present here, considering the site isn't run or hosted within that country so the only laws that apply should be native?

I think it's about the principle, the law is something that the world is looking at, the world will probably want it after they see the quality it brings but companies are skeptical because of the work it forces you to do and to what cost. As you maybe noticed people are skeptical because they think it doesn't bring "that" much to the table so why bother. Or at least i guess.

(Jun 26, 2018 06:57 PM)Enronitis Wrote: [\[CITE\]](#) Regardless, whether it ends up being good for the end user or not, its certainly screwing a lot of businesses and as mentioned, almost no one is technically fully "compliant" with many opting to jump ship completely.

Gotta love the law sometimes ?

Even if it is like you say "No one is techically fully compliant" which maybe is true to a degree but the main part is that people should reach/strive for the quality.

Enronitis - June 26, 2018, 7:25 pm

(Jun 26, 2018 07:08 PM)Silver Fang Wrote: [\[CITE\]](#) I think it's about the principle, the law is something that the world is looking at, the world will probably want it after they see the quality it brings but companies are skeptical because of the work it forces you to do and to what cost. As you maybe noticed people are skeptical because they think it doesn't bring "that" much to the table so why bother. Or at least i guess.

Even if it is like you say "No one is techically fully compliant" which maybe is true to a degree but the main part is that people should reach/strive for the quality.

I think for the most part, businesses and business owners ARE-

But the issue is some of the items are very vague to the extent we don't know if we are actually compliant or if we are moments away from receiving a crippling penalty.

overlude - June 26, 2018, 7:27 pm

Omniscient Wrote:You have full control by not joining. I stopped using my Facebook accounts a very long time ago. I am careful about sites I join and if I am worried about abuse of the information I give them then I don't join.

That's exactly what the GDPR addresses. As you understand, a lot of your (active) userbase involves kids. A lot are adults, but an alarming number will be < 18 I imagine, a majority < 21. This is a young age. The GDPR classes < 18s as vulnerable individuals, and they are. They have no clue what they're consenting to, or the importance of their data. I'm not sure I can say I did, and you perhaps can't say so either (ofc I can't comment on your behalf).

The people charging back on you may well be 13-17 years old. They don't know what they're doing, they perhaps don't see it as scamming, and in general they sure don't know what can happen to people on this site that "piss off" certain types. A policy of putting addresses in signatures puts them at risk. That, in my opinion, would be the most concerning policy of yours. They'll have other digital footprints anyway, any motivated individual can find them if they want, but my point is that these kids aren't always competent enough to engage on this site.

Even as adults, it's hard to know what you're getting into. A key aim of the GDPR is to make privacy

polices more verbose, so individuals signing up better know what they're getting into, and can not sign up if some of this info concerns them.

Even then, they can mess up and I don't think it's fair to have that looming over their heads forever. The previous data protection acts already had (rather absolute) rights to erasure if processing caused "significant duress". Generally speaking, I don't think a data controller should be processing information they have no reason to process other than for the sake of it.

You, yourself, realise now you don't want your data on Facebook (and you're in a rather unique position to care more about your privacy, I'd guess), others may take longer to realise that, perhaps not until after they've consented to processing. Also, sometimes we can't control who we have to give our data to. We may strictly speaking have the right to not use a service, but we're effectively blackmailed into using such service. An example is centralised application services for universities. We may not want them to process our data, but if an individual wants to get into X university they're effectively forced into it. Same goes for CRAs etc...

Omniscient Wrote:I assume you don't own a business or at least one that has to comply with GDPR.

I reside in Europe, and do run a business that needs to comply with the GDPR, processing more personal information than Hack Forums (based off what you've said). I also freelance for businesses processing sensitive information. My opinions of the GDPR are more following my personal opinions on individual rights to privacy.

The GDPR is stretched out of context. The rights offered are not absolute rights, and delving deeper into the legislation shows that. Before the GDPR, I've adhered to providing the same protections to users I would expect myself (and I expect a fair bit), so the main changes for me personally were mainly privacy policy changes to be more transparent. Complying with the GDPR is not a burden. If you look at headlines like "right to erasure" it may sound like it, but delving deeper you realise the GDPR is not there to make your life harder, it's there to make it harder for businesses that couldn't care less about personal (and perhaps sensitive) information about their users. That's wrong, with or without GDPR.

I have no problem with the additional burdens though. I went out of my way to do a fair bit of it regardless, and to me my customers having sufficient faith in my respect for their privacy is more important than some additional hours I 'waste' into ensuring those protections. I don't think any of them care tbh., but I would in their shoes so it's worth my time for me. I'm aware not all business owners feel this, though. None of my freelance clients share the same view and all of them viewed it as a burden. Some possess very sensitive information, so I find it very concerning that they don't view the GDPR as an opportunity. Perhaps I'm just the naive one here, though, since clearly nobody else views it in the ways I do.

Omniscient Wrote:There is a number of things written into GDPR which requires a lot of work on the part of businesses. Just trying to understand the full scope of this huge law and how it applies to your business is a vast undertaking. I am easily 50+ hours into my own research and implementation trying to be compliant. And I bet another 20-50 hours gets logged before this is done. I'm one small site, so imagine your a multinational corporation with thousands of employees. They not only have to comply but if they don't they do risk facing the \$20 million fine for each violation.

It's an easy law to understand but a difficult one to implement, admittedly. It's clear in the rights it wants to give and its purpose, as if it were a manifesto, but it isn't concrete in how businesses should reasonably implement these rights. That's the same for most EU legislation tbh, future legislation looks worse.

It's actually easier for the multinational corps imo, they have access to large consultancy firms that have interpreted the hell out of this for years. For places like Google they just had to deploy new privacy policies. Their operations haven't changed much from what I can tell. They (presumably) just found better ways to process data and have used the entire 2 year transition window for this.

Even then, even the data protection authorities aren't fully sure on the GDPR. There are inconsistencies in enforcement across the EU. The UK DPA says one thing, the Finnish one says another, and it's the DPAs that do enforcement in the first instance. The EU made this regulation up and forced it down on the member states to enforce, so it's not really the most centralised piece of legislation. The issue is that a complaint can be filed in any EU member state, so I'm not sure how jurisdiction works here when they themselves aren't 100% here.

Omniscient Wrote: I am listening to feedback and doing my absolute best to quote the actual law when I do interpret. I don't want to quote articles about the law or posts from the web. I prefer to read the law myself and use the words in it to justify my own policy. That's the only way imho we can be compliant.

The current agreement will likely be changed and updated and definitely the Help Doc will get completely rewritten too. Oh, we'll also be adding that little cookie popup thing soon too. More annoying crap.

I probably have read more about this law than a US lawyer. Also, I don't intend to keep addresses. I may have to go into some archive folders and just delete all my very old backups. I still have site files from 10 years ago, which I'm willing to bet most webmasters do that. You run backups, drop into folder, and forget it. No one puts an expiration date on files to self-delete. Agreed. You're the best person to understand your operations. It's hard to explain tech sites to traditional lawyers/firms (in my experience anyway). It's more just a case of checking your interpretations are valid and justifiable. At the end of the day, the people that would review violations think similar to the traditional firms providing consultancy. The EU is clearly out of the loop in tech, as evident by their copyright regulations they're cooking up. Some interpretations you find valid may not be is all, I ran my logic by someone as well and found some flaws, helps to have someone "experienced" check (although, they tend to hint that they're uncertain).

BTW, you may be able to keep those backups. The GDPR (and previous data protection acts) apply to sortable data. If you can run a search, or if data is categorised (either physically in a file and filing cabinet, or in a database) it falls under the GDPR. If it's stored in various backups over a long period I do not believe the GDPR reasonably requires you to delete or modify data from them all.

See: gdpr-info.eu/art-2-gdpr/

Quote: This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Of course this is ironic, because you can retain all the data you want in backups and if you really want some data you can fish it out of them. Recommendations here:

acronis.com/en-us/blog/posts/backups-and-gdpr-right-be-forgotten-recommendations

Seems to me like they would expect you to categorise individual data separately in backups so it's easily, widely, erasable but for prior backups they won't expect you to sort through and delete data. IANAL so YMMV.

Silver Fang - June 26, 2018, 7:31 pm

(Jun 26, 2018 07:25 PM) Enronitis Wrote: [\[CITE\]](#) I think for the most part, businesses and business owners ARE-

But the issue is some of the items are very vague to the extent we don't know if we are actually

compliant or if we are moments away from receiving a crippling penalty.

Ah yeah, at this point i don't think anyone would be fined. As i said earlier i think the law will be more specified with the time as it's needed to see what can be done and what should be done.

I don't think you have to worry that much at this point if you have done your best according to what the law actually states.

I'm pretty sure there is law-consultants for European companies that help to clarify the ongoing process for people.

What i also would like to know is how companies like Faceit / ESEA that have services which basically sniffing out a lot of information on what you are doing with your system how they are going to maintain their services if the GDPR law states that users are within their rights to know what information is gathered about you.

It's a direct conflict with Anti-cheats, Anti-Virus as they are there to protect you and to hide their detection strategies etc.

overlude - June 26, 2018, 7:48 pm

(Jun 26, 2018 07:31 PM)Silver Fang Wrote: [\[CITE\]](#) What i also would like to know is how companies like Faceit / ESEA that have services which basically sniffing out a lot of information on what you are doing with your system how they are going to maintain their services if the GDPR law states that users are within their rights to know what information is gathered about you.

It's a direct conflict with Anti-cheats, Anti-Virus as they are there to protect you and to hide their detection strategies etc.

ESEA has already seen the consequence of disobeying EU regulations despite being in the US. If you haven't noticed, they finally charge EU customers VAT now, they wrote about it on their blog a year ago. I have no doubt that they intend to fully comply with the GDPR if they haven't already. FACEIT is a UK corporation anyway, so they're under direct EU authority.

They are allowed to process data with consent or for "legitimate business interests" btw. Both reasons fit processing data for the purposes of anti-cheat behaviour. I presume they use "legitimate business interests" though, since this allows you to keep processing even if the user withdraws consent. Key note on this condition, such business interests must not override the legitimate privacy interests of the data subject.

FACEIT: Quote:We also collect Personal Information to investigate complaints of cheating or behavior that we believe may be contrary to our T&C, including the Code of Conduct. This may include screenshots of players' computer desktops or footage of in-game play.

ESEA: Quote:Anti-cheat functionality in the ESEA Client. Certain information regarding your computer and software it contains is required for effective operation of our anti-cheat services. By using the ESEA Client, you consent to the collection and analysis of information from your computer that ESEA deems reasonably necessary to identify and prevent the use of cheat software, files used to gain an unfair advantage, and to enforce bans. This information collection is not strictly limited to when you are logged in to the ESEA Client. Information analyzed or collected by the ESEA Client may include hardware, network and software identifiers; running programs; system configuration information; files or data suspected of being used to cheat or gain an unfair advantage; or screenshots while you are logged in and playing a game through the ESEA Client.

This is a vague interpretation, I haven't bothered read the full policy but I presume this falls under the legitimate business interests stuff. I'd say it counts. The GDPR doesn't stop you processing data, just means you have to be more transparent about it, and only process it if you need to, or if the user allows you to (amongst some other reasons that may be more applicable for some contexts).

Enronitis - June 26, 2018, 7:51 pm

(Jun 26, 2018 07:31 PM)Silver Fang Wrote: [\[CITE\]](#) Ah yeah, at this point i don't think anyone would

be fined. As i said earlier i think the law will be more specified with the time as it's needed to see what can be done and what should be done.

I don't think you have to worry that much at this point if you have done your best according to what the law actually states.

I'm pretty sure there is law-consultants for European companies that help to clarify the ongoing process for people.

What i also would like to know is how companies like Faceit / ESEA that have services which basically sniffing out a lot of information on what you are doing with your system how they are going to maintain their services if the GDPR law states that users are within their rights to know what information is gathered about you.

It's a direct conflict with Anti-cheats, Anti-Virus as they are there to protect you and to hide their detection strategies etc. My company looked into talking to European firms, and a couple of them were just as knowledgeable as most American firms, if not less so in some cases.

One firm we contacted basically shrugged their shoulders verbally saying "We are still working on that"-

That's scary.

ESEA/FACEIT/ETC will need to have extremely lengthy agreement policies, and take the appropriate measures to store all that data in a secure, and easily purged format. I imagine that they will be able to mask strategies to some extent as I can't imagine user movements are permanently stored, or would ever need to be. Temporary data like that can be auto-purged, so upon request there would be nothing there anyway.

Cyber Coder - June 27, 2018, 5:28 am

i am curious , if some government agency asks about an account, are you willing to share a user sensitive data with them WITHOUT any warrant ?

lolbott - October 27, 2019, 12:31 am

I just got a pop up about GDPR even I logged in couple weeks ago without being prompted about this and now I see that this thread is created back in 2018:

Quote:General Data Protection Regulation (GDPR) Compliance:

You agree that you're at least 16 years old if you are a resident or citizen of the European Union. Non-EU residents agree that they are a minimum age of 13.

You agree to use a pseudonym username that does not associate to your personal information. This includes, but is not limited to, association with social media accounts, websites you own or manage, ethnicity, location, school, workplace, emails accounts or your real name.

You agree that your posts will not contain information which may expose personally identifying information.

You agree that your profile signature, avatar, and other account editable data will not contain information that will identify you.

You agree that all data you submit to our website will not identify you and that we are not obligated to remove it based on personal privacy.

You agree that you will not post information which might identify another person. This includes but is not limited to emails, social media accounts, addresses, screenshots, or real names.

You agree that all posts and content posted meets the standard for "important public interests" or "journalism" and as such will not be required to be altered or deleted.

You agree that if you participate in using our website for deals, trades, sales, and other market activity that your personal information may be stored and even exposed for the purpose preventing, investigating, detecting, and prosecution of legal responsibility and liability in both civil and criminal law.

You agree that our storage method of your data is within reason. Personal data is retained for a period up to 7 years and is stored in a database format accessible directly only by the administrators.

You consent that Staff group members may have access to the IP address of all posts, your registration IP, and your recently used IP.

You consent that Admin group members may have access to any IP address you've used on the site, your email address, and can have read access to your private message folders.

You agree that the exposure of your IP address to Staff and Admin group members is reasonable for site function.

You consent that site backups may be kept for up to a 6 month period and done on a daily basis. The stored information is only for site backup and recovery purposes and the data is not sold or shared and is kept securely according to internet standards on cloud datacenters.

You consent that data we have stored on your account may be downloaded only once per 30 day period. This will provide you the most accurate results of what we have stored. Data exports manually done more than once per 30 days will incur a \$10 fee for processing.

You agree that your account may only be self-deleted if no posts are made.

You agree that in the event of a server change the data we store may be securely moved to a new location. We agree to inform you of a data move at least 3 days prior and provide you the option to close your account beforehand.

You agree that if you are not an EU citizen or resident that you do not fall under the GDPR (General Data Protection Regulation) law. Citizens and residents of the EU may be required to prove your citizenship or residency to provide you the legal protections and rights of that law.

You agree that for our service to function correctly your IP address and browser information may be shared with our vendors such as Cloudflare.

You agree that for our email service to function correctly your IP address and email information may be shared with our email vendor Elastic Email. We agree not to sell your email.

We are not interested to know who you are. You should not reveal your real identity to members. Your participation on our forum should be done from an anonymous and privacy perspective. We agree to not share or sell your data with 3rd parties. This webpage informs all visitors of current policies and is kept current. Only those who consent and agree to site policies will be allowed site access.

Was this prompt enforced back in 2018 or in past the few weeks?

spiral - October 27, 2019, 2:56 am

(Oct 27, 2019 12:31 AM)lolbott Wrote: [\[CITE\]](#) I just got a pop up about GDPR even I logged in couple weeks ago without being prompted about this and now I see that this thread is created back in 2018:

Was this prompt enforced back in 2018 or in past the few weeks?
I remember it being enforced last year

Omniscient - October 27, 2019, 11:44 am

(Oct 27, 2019 12:31 AM)lolbott Wrote: [\[CITE\]](#) I just got a pop up about GDPR even I logged in couple weeks ago without being prompted about this and now I see that this thread is created back in 2018:

Was this prompt enforced back in 2018 or in past the few weeks?
It's part of policy. If you haven't logged in since this was enacted then that's why it prompted you.

lurking - October 27, 2019, 1:29 pm

Thank you for your continued work and public disclosure of your assessment and implementation of GDPR on HF. You provide an example for other websites, smaller forums, less experienced webmasters/owners, etc to be able to compare to.

Something that is very appreciated.