NEEYAMO

Impact of GDPR in the world of Background Verification.

#WithNeeyamo

"organizations and applicants insist on knowing all data handling touch-points which is now become a new normal."

#BackgroundVerification #WithNeeyamo

#WITHNEEYAMO

It has been a while now since the enforcement of GDPR, what in your view has been the biggest impact of GDPR in the world of Background Screening?

There are two angles from which one can assess this impact,

A - The consumer of the screening services, i.e, applicants and organizations who benefit from the results of employee screening

B - Background Screening organizations.

Organizations have become increasingly aware of laws and regulations surrounding privacy due to the onset of GDPR. Customers insist that their data resides in EU Economic area. Organizations are witnessing instances where applicant deny consent for performing specific checks. The repercussions for this denial has seen a tremendous shift when compared to hiring decisions taken pre-GDPR. While denial of consent was earlier regarded as a threat (companies could site this as a reason to deny employment), the GDPR has now provided this as an alternate course for applicants without having to face the risk of loosing their chances to work with the organization.

Furthermore, organizations and applicants insist on knowing all data handling touch-points which is now become a new normal.

Talking about the impact of GDPR among background screening companies; I would say the biggest impact has been to ensure that organizations realign their privacy framework inorder to align with the norms set forth by GDPR. In a few cases, background screening companies have had to build their framework from ground-up by using their own expertise or by having employed external consulting agencies. In addition to this, customers of background screening companies have increasingly insisted on service provider audits to be conducted inorder to validate compliance to norms put forth by the GDPR.

Do you foresee any increase in the operating cost of performing Background Check due to the impact of GDPR? If yes, can you throw some light?

Yes. There is a definite increase in the operating cost post implementation of GDPR. The cost may vary for each organization depending upon the changes they have had to make. The major contributing factor for this increase in cost has been due to legal consultations which include reviewing and updating contractual documents, privacy policies, setting up a helpdesk to answer privacy related queries or complaints.

Secondly, screening providers have had to invest to additional due-delligence on their sub-contractors who service their requirements for the EU region. The appointment of the DPO has been an additional expense for organizations as this appointment is a requirement put forth by the GDPR.

The third cost factor has certainly been the focus on the IT infrastructure, specifically due to restrictions imposed to ensure data of EU members reside within the EU Econimic Area due to which organizations have had to take adequate steps to abide by this requirement. In addition to this, implementing data security technology such as Pseudonymization, anonymization, encryption, data backup have contributed to increased costs.

"From an employee stand-point, the Background Screening process can be distinguished in three aspects – Consent, Information & Technology."

#BackgroundVerification #WithNeeyamo

#WITHNEEYAMO

Can an employee's data be transferred outside the EU Economic Area while performing Background Screening?

Yes, the data can be transferred outside the EU Economic area, by implementing appropriate technical and administrative safeguards.

Another important requirement is to obtain explicit consent by the data subject to facilitate cross border transfer of their personal data.

If these conditions are met, then data can be transferred outside EU.

Do you think adopting automation in Background Screening can help combat challenges faced due to GDPR?

Technology has always played a major role in streamlining and optimizing any HR process and Background Screening is no exception.

Automating the Background Screening process will prevent manual intervention to a larger extent thereby maintaining data integrity and confidentiality.

Having your Background Screening system hosted in one of the EU regions is a definite add-on to ensure adherence to compliance.

Providers like Neeyamo have their Background Screening system hosted in the EU region (https://bit.ly/2IBP87v) that enables them to provide unhindered Background Screening services.

From an employee's stand-point, what factors should one keep in mind while performing Background Screening in the EU region?

From an employee's stand-point, the Background Screening process can be distinguished in three aspects – Consent, Information & Technology.

It is important for an employee to be aware that Background Screening cannot be carried out without his/her prior consent.

GDPR allows employees to object to background screening at any given point of time – even if it's accuracy is not contested

It is also interesting to note that an employee has all the right to request for a consent form in their preferred language.

Moving to Information – employees are expected to provide their information with utmost accuracy and on-time .

Delays in providing the required information or willfully providing incorrect information has a huge impact on the Background Screening results.

Background Screening providers these days have started leveraging technology that are extremely user-friendly. A provider owned screening portal with an engaging UI would encourage employees to upload/update relevant information and further fasten the Background Screening process .

Could you list few best practices for a Background Screening provider while dealing with the changes due to the impact of #GDPR #WithNeeyamo ?

To begin with the basics – your Privacy policy should include all the required terms and norms defined by GDPR (e.g. https://bit.ly/2IDF0Lu)

It would be my strong recommendation to providers to record proof of consent

"Companies can be imposed a fine of either 4% of their annual revenue or 20 million Euros, whichever is higher"

#BackgroundVerification #WithNeeyamo

#WITHNEEYAMO

obtained from employees for carrying out their Background Screening process.

If one engages a sub-contractor, it is now more crucial than ever to ensure their data security policies & procedures are in accordance with the GDPR norms. Request for a thorough health check on your partner's readiness and request for periodic audits and reports.

One can always create a detailed process – Understand, Implement and Monitor to help keep abreast of the changes in regulations and norms .

Knowledge is power - the most powerful tool has to be the screening team who should be trained to deliver accurate reports.

Lastly, what are the consequences of non-compliance to #GDPR regulations?

The impact of non-compliance to GDPR regulations are both tangible as well as intangible in nature. The company also stands to risk its reputation & brand in the process.

Speaker

Shraddha Deshpande

Head - Implementation, Partnership Alliance & Compliance for Background Verification at Neeyamo

We are listening!

Mail us : irene.jones@neeyamo.com

Call us : +1 888 9 NEEYAM

www.neeyamo.com

www.linkedin.com/company/Neeyamo

www.twitter.com/Neeyamo

www.facebook.com/Neeyamo