



Classification: Public

PERSONAL DATA PROTECTION NOTICE

Personal Data Protection Act 2010 ("**PDPA 2010**"),

This notice ("**Notice**") is issued by **VENOVox SDN BHD** and its group of companies operating in Malaysia, Singapore, and the UK (collectively referred to herein as "**we**", "**us**", "**our**", "**Venovox**" or "**Data Processor**"). Venovox provides a comprehensive screening and background reports for our clients (collectively referred to herein as "**client**" or "**Data Controller**"). For the purpose of this Notice, words and expressions used herein shall, unless otherwise defined, have the meanings ascribed to them under the PDPA 2010.

By signing the corporate background screening consent form, submitting information to us or interacting with us in any way, you agree and consent to us collecting, using, processing and disclosing your personal data in the manner set forth in this Notice.

1. The processing of personal data

- (a) For the purpose of the processing of personal data, we will be collecting your data comprising of your name, National Identity Registration Card number, Passport Number, all information within your CV, degree/qualification certificate, and other the personal data which forms the search scope on a case-to-case basis.
- (b) Our search scope encapsulates both personal data and sensitive personal data. Sensitive personal data is defined as any personal data consisting of information as to the physical or mental health or condition (e.g. health assessments) of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence (e.g. Reputational Risk Report, Civil & Criminal Prosecution searches, etc.) biometric data or any other personal data as the Minister may determine by order published in the Gazette.

By signing the corporate background screening consent form, undergoing health assessment checks with us, or voluntarily submitting sensitive personal data to us, you consent to us collecting, using, disclosing and sharing your sensitive personal data, and disclosing such personal data to authorised service providers and/or relevant third parties in the manner set forth in this Notice.

- (c) If you provide us with any personal data relating to a third party (e.g., information of your spouse, children, parents, and/or employees), you
- (d) represent to us that you have obtained the consent of such third party to provide us with their personal data for the respective purposes and further processing.



Classification: Public

- (e) We will not knowingly collect or process personal data of individuals under the age of 18 without the prior consent of their parent or legal guardian. By providing us with personal data of individuals under the age of 18, you consent or represent to us that you have obtained the consent of the parent or legal guardian of the minor to the collection, use, processing and disclosure of the personal data of the minor.

2. The need for processing

- (a) The personal data compiled is solely for the purpose of generating a Venovox Report for our clients as the Data Controller. The use of Venovox Report is predominantly to assist the Data Controller with making employment decisions.
- (b) Your personal data will be retained by us until a Venovox Report is generated. Our turnover time ranges from 2 days to 7 days.
- (c) Upon the 180th day the Venovox Report is generated (calculated from and including the day Venovox Report is delivered to our client via the “hi – by Venovox” portal), your personal data will be permanently deleted from our system, and we will not retain any copy of the Venovox Report, unless agreed otherwise through written agreement.
- (d) We will take reasonable measures to ensure that the personal data that we have in our possession is secured. Measures taken includes the following:

Access Control

Personal data is encrypted at rest and access is governed by role-based controls within our systems. Administrative access to servers and management systems is restricted to authorised personnel only, protected by multi-factor authentication and access credential policies. Access rights are reviewed periodically and revoked promptly when no longer required.

Data Transmission Security

All personal data transmitted through our web applications and services is secured using HTTPS (SSL/TLS encryption) to prevent unauthorised interception or tampering during transit.

Server & Infrastructure Security

Our systems are hosted on cloud infrastructure with industry-standard physical and logical security controls. Firewall configurations, regular security patching, and software updates are applied on an ongoing basis to reduce exposure to known vulnerabilities.



Classification: Public

System Monitoring & Maintenance

We conduct routine system monitoring, including log review and activity auditing, to detect and respond to suspicious or anomalous behavior. Systems are regularly maintained to ensure they remain secure and up to date.

Incident Response & Breach Notification

To ensure our response capabilities remain effective, we conduct annual breach simulation exercises and perform recovery testing on our Disaster Recovery (DR) environment to validate our preparedness and minimise potential disruption to operations and data integrity.

3. The source of personal data gathered

- (a) Personal data is collected from internal sources (e.g., application forms, internal systems) and external sources (e.g., third-party providers, employers (past, current and future), institutions, person you have authorised to provide us with your personal data, and public/regulatory databases), via both manual and digital means.

4. Data subject rights

- (a) You should ensure that all personal data submitted to us is complete, accurate, true and correct. Failure on your part to do so may result in inaccuracy or incomplete Venovox Report, which may affect our client's decision to make an employment offer to you or to maintain your employment with them. It is mandatory for you to provide the requested personal data in order for us to deliver our services which our client had ordered. Failure to provide any personal data requested will limit, delay, or otherwise affect our ability to provide our services or to respond effectively to your requests, enquiries, or applications.
- (b) At all times, you have the right to access and request a copy of your personal data. Please do not hesitate to reach out to Venovox in accordance with paragraph 4 (f) below should you wish to exercise this right. However, we will only be able to furnish a copy of the requested document in digital form, in compliance with our ESG policy.
- (c) At all times, you have the right to correct or update your personal data. Please do not hesitate to reach out to Venovox in accordance with paragraph 4 (f) below should you wish to exercise this right.
- (d) At all times, you have the right to give consent to, or to withdraw your consent to all or parts of the collection and/or disclosure of your personal data. Please



Classification: Public

do not hesitate to reach out to Venovox in accordance with paragraph 4 (f) below should you wish to exercise this right. However, do take notice of the repercussion of your withdrawal as elaborated under paragraph 4 (a) above.

- (e) In order to process any of your requests under this paragraph 4, we may request for additional information in order to verify your identity. We reserve the right to reject any of your request if we are unable to verify your identity or where it is allowed by the law.
- (f) For the purpose of the abovementioned paragraphs 4 (b) to 4 (d), kindly reach out to us through our Legal Counsel cum Data Protection Officer, See Tian Xin at our Global WhatsApp Number +6012 800 8888 or via email at dpo@venovox.com. Our research analysts are also readily available to assist you via the communication log in the “Hi” Portal.

5. The disclosure of personal data

- (a) Personal data may be disclosed to authorised third parties which may be located within or outside of Malaysia strictly for the purpose of fulfilling verification, screening, and compliance requirements. These include:
 - (i) **Our affiliate companies:** To provide you or our client with our services
 - (ii) **Your previous or present employers:** To verify employment history
 - (iii) **Educational institutions:** To verify academic qualifications
 - (iv) **Referees:** To obtain character and performance references
 - (v) **Regulatory and governmental authorities:**
Where required for compliance with applicable laws and regulations
 - (vi) **Third-party service providers / verification partners / Private and public sector repositories of information / Credit Bureaus:** To perform specific checks (e.g., criminal record searches, credit-related checks, sanctions screening)
 - (vii) **Any other person, organisation or agency possessing relevant information about you:** To perform specific checks

All disclosures are limited to data necessary for the intended purpose and are carried out with appropriate authorisation and/or consent from the data subject, in line with the PDPA 2010.



Classification: Public

By signing the corporate background screening consent form or continuing to engage with us, you are deemed to have consented to the disclosure and cross-border transfer (where applicable) of your personal data to the third parties listed above, whether within or outside of Malaysia, where such disclosure or transfer is necessary to fulfil the purposes listed in this Notice.

- (b) Appropriate technical and organisational security measures are implemented to ensure that all disclosures of personal data are conducted in a secure manner, including:
 - (i) **Data encryption and password protection** (e.g., encrypted files and secure transfer protocols)
 - (ii) **Access controls and role-based permissions** to restrict data access to authorised personnel only
 - (iii) **Secure communication channels** (e.g., company portal, secure email, or encrypted file-sharing platforms)
 - (iv) **Confidentiality agreements and due diligence** for all third-party service providers
 - (v) **Data minimisation principles**, ensuring only necessary data is disclosed
 - (vi) **Audit trails and logging** to monitor and track data disclosures
 - (vii) **Alignment with information security standards such as ISO/IEC 27001:2022**

6. Version

This Notice is issued in both English and Bahasa Malaysia languages. In the event of any inconsistency, the English language version of this Notice shall prevail.

Effective Date: 01.07.2026

Last Review Date: 10.08.2026



Classification: Public

NOTIS PERLINDUNGAN DATA PERIBADI

Akta Perlindungan Data Peribadi 2010 ("APDP 2010"),

Notis ini ("**Notis**") diisukan oleh **VENOVox SDN BHD** dan Kumpulan syarikatnya yang beroperasi di Malaysia, Singapura dan UK (dirujuk secara kolektifnya sebagai "kami", "kita", "Venovox" atau "Pemproses Data"). Venovox menyediakan perkhidmatan saringan yang menyeluruh dan laporan latar belakang bagi pelanggan kami (dirujuk sebagai "pelanggan" atau "Pengawal Data"). Bagi tujuan Notis ini, perlataan dan ungkapan yang digunakan membawa maksud seperti yang ditafsirkan di bawah APDP 2010 melainkan yang ditafsirkan sebaliknya.

Dengan menandatangani borang persetujuan saringan latar belakang korporat, mengemukakan maklumat kepada kami atau berinteraksi dengan kami dalam apa jua cara, anda dianggap bersetuju dan memberi kebenaran kepada kami untuk mengumpul, menggunakan, memproses dan mendedahkan data peribadi anda sebagaimana dinyatakan dalam Notis ini.

1. Pemprosesan data peribadi

- (a) Bagi tujuan pemprosesan data peribadi, kami akan mengumpul data anda yang merangkumi nama, nombor Kad Pengenalan, nombor pasport, semua maklumat dalam CV anda, sijil ijazah/kelayakan, serta data peribadi lain yang termasuk dalam skop carian berdasarkan kes.
- (b) Skop carian kami merangkumi data peribadi dan data peribadi sensitif. Data peribadi sensitif ditafsirkan sebagai data peribadi yang mengandungi maklumat tentang kesihatan atau keadaan fizikal atau mental (contohnya penilaian kesihatan) seorang subjek data, pendapat politiknya, kepercayaan agamanya atau kepercayaan lain yang bersifat seumpamanya, pelakuan atau pengataan pelakuan apa-apa kesalahan olehnya, data biometrik atau apa-apa data peribadi lain yang ditentukan oleh Menteri melalui perintah yang disiarkan dalam Warta.
- (c) Dengan menandatangani borang persetujuan saringan latar belakang, menjalani pemeriksaan kesihatan dengan kami, atau secara sukarela mengemukakan data peribadi sensitif kepada kami, anda dianggap memberi persetujuan kepada kami untuk mengumpul, menggunakan, mendedahkan dan berkongsi data peribadi sensitif anda kepada penyedia perkhidmatan yang diberi kuasa dan/atau pihak ketiga yang berkaitan seperti yang dinyatakan dalam Notis ini.
- (d) Sekiranya anda memberikan data peribadi pihak ketiga (contohnya data pasangan, anak, ibu bapa dan/atau pekerja), anda mengesahkan bahawa anda telah mendapatkan persetujuan pihak berkenaan untuk memberikan data mereka kepada kami untuk tujuan yang dinyatakan.



Classification: Public

- (e) Kami tidak akan mengumpul atau memproses data peribadi individu di bawah 18 tahun tanpa persetujuan ibu bapa atau penjaga sah. Dengan memberikan data sedemikian, anda mengesahkan bahawa persetujuan ibu bapa atau penjaga sah telah diperoleh.

2. The need for processing

- (a) Data peribadi yang dikumpul adalah semata-mata untuk tujuan menghasilkan Laporan Venovox bagi pelanggan kami sebagai Pengawal Data, terutamanya untuk membantu membuat keputusan dari segi pekerjaan.
- (b) Data peribadi anda akan disimpan sehingga Laporan Venovox dihasilkan dalam tempoh 2 hingga 7 hari.
- (c) Pada hari ke-180 Laporan Venovox dihasilkan (dikira dari dan termasuk hari Laporan Venovox dihantarkan kepada pelanggan kami melalui portal “*hi - by Venovox*”), data peribadi anda akan dipadamkan secara kekal daripada system kami, dan kami tidak akan menyimpan sebarang Salinan Laporan Venovox kecuali seperti yang dipersetujui melalui perjanjian bertulis.
- (d) Kami akan mengambil Langkah-langkah yang munasabah untuk memastikan keselamatan data kami. Langkah-langkah yang telah diambil termasuk:

Kawalan Akses

Data peribadi disulitkan (*encrypted*) semasa disimpan dan akses dikawal oleh kawalan berasaskan peranan dalam sistem kami. Akses pentadbiran ke pelayan dan sistem pengurusan hanya terhad kepada kakitangan yang dibenarkan, dilindungi oleh pengesahan berbilang faktor dan dasar kelayakan akses. Hak akses disemak secara berkala dan dibatalkan dengan segera apabila tidak lagi diperlukan.

Keselamatan Penghantaran Data

Semua data peribadi yang dihantar melalui aplikasi dan perkhidmatan web kami dijamin (*secured*) menggunakan HTTPS (penyulitan SSL/TLS) untuk mengelakkan pintasan atau pengubahan tanpa kebenaran semasa transit.

Keselamatan Pelayan & Infrastruktur

Sistem kami dihoskan pada infrastruktur awan dengan kawalan keselamatan fizikal dan logik standard industri. Konfigurasi *firewall*, penampalan keselamatan berkala dan kemas kini perisian digunakan secara berterusan untuk mengurangkan pendedahan kepada kelemahan yang diketahui.



Classification: Public

Pemantauan & Penyelenggaraan Sistem

Kami menjalankan pemantauan sistem rutin, termasuk semakan log dan pengauditan aktiviti, untuk mengesan dan bertindak balas terhadap tingkah laku yang mencurigakan atau anomali. Sistem diselenggara secara berkala bagi memastikan ia kekal selamat dan terkini.

Pemberitahuan Tindak Balas Insiden & Kebocoran

Bagi memastikan keupayaan tindak balas kami kekal berkesan, kami menjalankan latihan simulasi kebocoran tahunan dan menjalankan ujian pemulihan pada persekitaran Pemulihan Bencana (DR) kami untuk mengesahkan kesediaan kami dan meminimumkan potensi gangguan kepada operasi dan integriti data.

3. Sumber data peribadi yang dikumpul

Data peribadi dikumpul daripada sumber dalaman (cth., borang permohonan, sistem dalaman) dan sumber luaran (cth., penyedia pihak ketiga, majikan (masa lalu, semasa dan akan datang), institusi, orang yang anda telah beri kuasa untuk memberikan kami data peribadi anda, dan pangkalan data awam/peraturan), melalui cara manual dan digital.

4. Hak subjek data

- (a) Anda harus memastikan bahawa semua data peribadi yang diserahkan kepada kami adalah lengkap, tepat, benar dan betul. Kegagalan anda berbuat demikian boleh mengakibatkan ketidaktepatan atau Laporan Venovox tidak lengkap, yang mungkin menjejaskan keputusan pelanggan kami untuk membuat tawaran pekerjaan kepada anda atau mengekalkan pekerjaan anda dengan mereka. Anda wajib memberikan data peribadi yang diminta agar kami dapat memberikan perkhidmatan yang telah dipesan oleh pelanggan kami. Kegagalan untuk memberikan sebarang data peribadi yang diminta akan menjejaskan, melambatkan atau menjejaskan keupayaan kami untuk menyediakan perkhidmatan kami atau untuk bertindak balas dengan berkesan terhadap permintaan, pertanyaan atau permohonan anda.
- (b) Pada setiap masa, anda berhak untuk mengakses dan meminta salinan data peribadi anda. Sila menghubungi Venovox mengikut perenggan 4(f) di bawah sekiranya anda ingin melaksanakan hak ini. Walau bagaimanapun, kami hanya akan dapat memberikan salinan dokumen yang diminta dalam bentuk digital, selaras dengan dasar ESG kami.
- (c) Pada setiap masa, anda berhak untuk membetulkan atau mengemas kini data peribadi anda. Sila menghubungi Venovox mengikut perenggan 4(f) di bawah sekiranya anda ingin melaksanakan hak ini.



Classification: Public

- (d) Pada setiap masa, anda berhak untuk memberi persetujuan atau menarik balik persetujuan anda terhadap semua atau sebahagian daripada pengumpulan dan/atau pendedahan data peribadi anda. Sila hubungi Venovox mengikut perenggan 4(e) di bawah sekiranya anda ingin melaksanakan hak ini. Walau bagaimanapun, sila ambil perhatian tentang akibat penarikan balik anda seperti yang dihuraikan di bawah perenggan 4(a) di atas.
- (e) Untuk memproses mana-mana permintaan anda di bawah perenggan 4 ini, kami mungkin meminta maklumat tambahan untuk mengesahkan identiti anda. Kami berhak untuk menolak mana-mana permintaan anda sekiranya kami tidak dapat mengesahkan identiti anda atau jika dibenarkan oleh undang-undang.
- (f) Bagi tujuan perenggan 4(b) hingga 4(d) yang dinyatakan di atas, sila hubungi kami melalui Penasihat Undang-undang dan Pegawai Perlindungan Data kami, See Tian Xin melalui Nombor WhatsApp Global kami +6012 800 8888 atau melalui e-mel di dpo@venovox.com. Penganalisis penyelidikan kami juga sedia membantu anda melalui log komunikasi dalam Portal “Hi”.

5. Pendedahan data peribadi

- (a) Data peribadi boleh didedahkan kepada pihak ketiga yang dibenarkan yang mungkin berada di dalam atau di luar Malaysia hanya untuk tujuan memenuhi keperluan pengesahan, penyaringan dan pematuhan. Ini termasuk:
 - (i) **Syarikat sekutu (affiliate) kami:** Untuk menyediakan perkhidmatan kami kepada anda atau pelanggan kami
 - (ii) **Majikan anda sebelum ini atau sekarang:** Untuk mengesahkan sejarah pekerjaan
 - (iii) **Institusi pendidikan:** Untuk mengesahkan kelayakan akademik
 - (iv) **Perujuk:** Untuk mendapatkan rujukan watak dan prestasi
 - (v) **Pihak berkuasa dan kerajaan:**
Di mana diperlukan untuk pematuhan undang-undang dan peraturan yang terpakai
 - (vi) **Penyedia perkhidmatan pihak ketiga / rakan kongsi pengesahan / Repositori maklumat sektor swasta dan awam / Biro Kredit:**
Untuk melaksanakan pemeriksaan khusus (cth., carian rekod jenayah, pemeriksaan berkaitan kredit, pemeriksaan sekatan)



Classification: Public

- (vii) **Mana-mana orang, organisasi atau agensi lain yang mempunyai maklumat berkaitan tentang anda:** Untuk menjalankan pemeriksaan khusus

Semua pendedahan adalah terhad kepada data yang diperlukan untuk tujuan yang dimaksudkan dan dijalankan dengan kebenaran dan/atau persetujuan yang sewajarnya daripada subjek data, selaras dengan APDP 2010.

Dengan menandatangani borang kebenaran saringan latar belakang korporat atau meneruskan berurusan dengan kami, anda dianggap telah bersetuju dengan pendedahan dan pemindahan merentas sempadan (jika berkenaan) data peribadi anda kepada pihak ketiga yang disenaraikan di atas, sama ada di dalam atau di luar Malaysia, di mana pendedahan atau pemindahan tersebut diperlukan untuk memenuhi tujuan yang disenaraikan dalam Notis ini.

- (b) Langkah-langkah keselamatan teknikal dan organisasi yang sesuai telah dilaksanakan bagi memastikan semua pendedahan data peribadi dijalankan dengan cara yang selamat, termasuk:
- (i) **Penyulitan data dan perlindungan kata laluan** (cth., fail yang disulitkan dan protokol pemindahan selamat)
 - (ii) **Kawalan akses dan kebenaran berasaskan peranan** untuk menyekat akses data kepada kakitangan yang diberi kuasa sahaja
 - (iii) **Saluran komunikasi yang selamat** (cth., portal syarikat, e-mel yang selamat atau platform perkongsian fail yang disulitkan)
 - (iv) **Perjanjian kerahsiaan dan usaha yang wajar** untuk semua penyedia perkhidmatan pihak ketiga
 - (v) **Prinsip pengurangan data (*Data minimisation principles*)**, memastikan hanya data yang diperlukan didedahkan
 - (vi) **Jejak audit dan *logging*** untuk memantau dan menjejaki pendedahan data.
 - (vii) **Penjajaran dengan piawaian keselamatan maklumat seperti ISO/IEC 27001:2022**



Classification: Public

6. Versi

Notis ini dikeluarkan dalam kedua-dua bahasa Inggeris dan Bahasa Malaysia. Sekiranya terdapat sebarang percanggahan, versi Bahasa Inggeris Notis ini akan diguna pakai.

Tarikh Kuat Kuasa: 01.07.2026

Tarikh Semakan Terakhir: 10.08.2026