TOL

To verify compliance with the regulations listed in the PIPL's Chapter 2 (Articles 13–17) based on the provided privacy policy, we will check specific key principles. Below is the verification:

### **Article 13 - Conditions for Processing Personal Information**

Requirement:
Personal information must be processed under one of the following lawful conditions:
1. Obtaining the individual's consent.
2. Necessary for contract performance or human resource management.
3. Compliance with legal duties or obligations.
4. Emergency protection of life, health, property during public health events.
5. For public interest purposes, i.e., news reporting.
6. Handling publicly disclosed information within reasonable limits or legally disclosed information.
7. Other circumstances specified by laws or regulations.

Privacy Policy Compliance:
- The privacy policy indicates that personal information is processed based on user consent and outlines the circumstances where consent is not required (e.g., complying with legal obligations, contract fulfillment, or public safety). It also includes provisions for handling publicly disclosed information.
✔ **Complies with Article 13**

### **Article 14 - Requirements for Consent**

Requirement:
Consent must be informed, voluntary, and explicit. Any changes to the purpose, method, or type of information processed require obtaining new consent.

Privacy Policy Compliance:
- The policy clearly states that consent must be obtained, especially for sensitive functions or device permissions. Explicit re-consent is required for new purposes or changes in the scope of processing. Consent is sought via pop-ups for sensitive device permissions.
✔ **Complies with Article 14**

### **Article 15 - Withdrawal of Consent**

Requirement:
Individuals have the right to withdraw consent at any time. Withdrawal does not affect processing actions already undertaken.

Privacy Policy Compliance:
- A withdrawal mechanism is outlined (e.g., turning off permissions or deleting accounts). The policy explicitly states that withdrawal does not impact past processing activities conducted under prior consent.
✔ **Complies with Article 15**

### **Article 16 - Non-Coercion in Consent**

Requirement:
Organizations cannot refuse services solely because an individual does not consent to the processing of personal information unless it's necessary for providing the service.

Privacy Policy Compliance:
- The policy ensures that refusing optional permissions does not impact access to basic features or services. Essential functions dependent on necessary data (e.g., providing a contact number) are reasonably justified.
✔ **Complies with Article 16**

### **Article 17 - Notification Requirements**

Requirement:
Prior to processing personal information, processors must notify individuals of:
1. Name and contact details of the processor.
2. Purpose, method, types of information, and retention period.
3. Method for exercising rights.
4. Any other matters required by law.

Changes to the above must be notified separately.

Privacy Policy Compliance:
- The privacy policy provides users with:
  1. Processor details and contact information (e.g., operator name, email, dedicated hotlines).
  2. Specific purposes, methods, types of information collected, retention periods, and options to modify or delete data.

3. Detailed sections on exercising rights (e.g., withdrawal, correction, deletion).
4. Procedures for notifying users about policy updates.
✔ **Complies with Article 17**

### **Conclusion**

Based on the provided privacy policy, all listed items in the document meet the requirements of Articles 13–17 of the PIPL. The privacy policy reflects compliance with informed consent, withdrawal mechanisms, notification obligations, lawful processing conditions, and non-coercion principles.

✔ **Overall: The privacy policy complies with the given PIPL regulations.**

NEU

Based on the provided regulations from the **Personal Information Protection Law (PIPL)** and the user privacy policy of the application, I will carefully examine compliance for sections relevant to Chapter 2 — Articles 13–17 of the PIPL. Here is the breakdown of the evaluation:

### **Compliance Analysis:**

#### **1. Article 13 — Grounds for Processing Personal Information**
Under Article 13, personal information can only be processed under specific circumstances, such as obtaining consent or legal, contractual, and public interest requirements.

- **Consent Requirement Fulfilled**:
  - The privacy policy explicitly states that **user consent is obtained** before accessing, collecting, or processing personal data for purposes like enabling device permissions, data collection, and other services. Sensitive permissions (e.g., camera, location) require separate pop-up requests.
  - Handling **important information like phone numbers for identity verification** aligns with legal and contractual obligations (e.g., network real-name regulations). If declined, users retain access to basic functionality, fulfilling the criteria under **(第二项 - Contract)**.

- **Special Situations Covered**:

  - Processing information for system security and troubleshooting falls under legal duties as per **(第三项 - Legal Duty)**.
  - The privacy policy includes sufficient explanation of reasons for retrieving user information for cyber-security purposes and fraud prevention mechanisms, aligning with regulatory standards under **(第十项)**.

✅ **Conclusion**: Complies with Article 13.

#### **2. Article 14 — Informed, Voluntary, Explicit Consent**
Consent must be informed with users knowing the full extent of data collection, processing purposes, and methods.

- **Detailed Transparency**:
  - The privacy policy provides clear explanations of how and why each **type of personal data** is collected (e.g., device permissions, search history, location).
  - It also informs users of changes to data processing purposes and requires **renewed user consent**, as per the regulation.

- **Voluntariness**:
  - Users can opt-out of non-essential data sharing or personalized features such as **algorithmic recommendations**, **marketing notifications**, and **profile visibility**.
  - Consent withdrawal mechanisms, such as **account settings** or **manual deletion processes**, are outlined.

✅ **Conclusion**: Fully compliant with Article 14.

#### **3. Article 15 — Consent Withdrawal**
Consent withdrawal mechanisms must be simple and feasible, ensuring it does not impair services beyond necessary functionalities.

- **Withdrawal Offered**:
  - Specific tools (e.g., account settings) allow users to withdraw permissions for items such as location services, personalized recommendations, and marketing communication consent.
  - In cases of withdrawal, services are **restricted strictly to necessary operations**, ensuring lawful compliance with **Article 15**.

- **Implementation Design**:
  - No penalization for withdrawal of non-essential permissions (e.g., marketing preferences would not affect access to browsing).

✅ **Conclusion**: Meets the requirements under Article 15.

#### **4. Article 16 — Unconditional Access Regardless of Consent**
Users cannot be denied products or services for refusing to provide consent, except where necessary processing directly relates to service provision.

- The policy allows **basic service functionality**, such as browsing and job application, without requiring additional personal data not essential to the core service (e.g., enabling location-based suggestions can be skipped).
- Declining permissions for personalized recommendations or external device permissions does not obstruct essential job-related services.

✅ **Conclusion**: Complies with Article 16.

#### **5. Article 17 — Information Disclosure Before Processing**
The privacy policy must provide users clear and detailed information on the entity processing their data, purposes, methods, and retention periods.

- **Information Provided**:
  - Detailed descriptions of processing methods, such as requirements for uploading job-seeking documents, identity verification for recruiters, and personalized recommendation algorithms.
  - A clear retention policy is addressed, allowing deletion or anonymization upon account termination or completion of processing purposes.

- **Entity Identification**:
  - The privacy policy discloses the processor's identity (北京华品博睿网络技术有限公司), contact information, and procedures for accessing or modifying personal data.

✅ **Conclusion**: Fully compliant with Article 17.

### **Key Strengths in Compliance:**
- Explicit transparency and consent mechanisms.
- Clear opt-out and consent withdrawal flows.
- Provisions for lawful processing without requiring unnecessary consent.
- Details on entity processing information and retention rules.

### **Potential Improvements:**

Although the policy meets the regulatory requirements, usability around access/removal requests (Article 17) could streamline further user interaction (e.g., automated processes instead of written requests).

### **Final Evaluation:**
The privacy policy for "BOSS直聘" **fully complies with Articles 13–17 of the Personal Information Protection Law (PIPL)** as outlined above. Both consent mechanisms and processing methods align well with the specified regulations.

AGG

To analyze whether the company's privacy policy adheres to the **Personal Information Protection Law (PIPL)** regulations, I will evaluate the provided privacy policy against the specified **PIPL regulations**. Here's the detailed analysis on each regulation:

### **Regulation Article 13: Conditions for Personal Information Processing**
Processing personal information requires either consent or falls within one of the specified exceptions.

- **Privacy Policy Compliance**:
  The company states it collects personal information based on user agreement and explains its purpose (e.g., registration, service optimization, legal requirements, etc.). Non-essential data is optional. Certain sensitive processing, such as real-name authentication, is tied to legal mandates (e.g., network real-name systems, labor management).
  - **Verdict**: Likely compliant. The privacy policy outlines lawful grounds for processing and allows users to opt-out of non-necessary features. However, more direct indication of lawful bases for exceptions needs clarification, indicating vigilance is required.

### **Regulation Article 14: Informed Consent**
Consent should be voluntary, explicit, and based on adequate information. Purpose, processing methods, and types of personal information must be disclosed, and any change requires renewed consent.

- **Privacy Policy Compliance**:
  It emphasizes informed consent through clear disclosure (e.g., processing requires device permissions, detailed descriptions of data use). Any purpose change prompts renewed consent. Sensitive permissions require pop-up dialog agreements.
  - **Verdict**: Likely compliant. The policy actively promotes informed consent. However, vigilance is required to verify implementation in practice.

### **Regulation Article 15: Withdrawal of Consent**
Users must be provided a convenient way to revoke consent. Withdrawal should not affect the efficacy of prior processing.

- **Privacy Policy Compliance**:
  Tools to withdraw consent are provided in app settings (e.g., disable permissions, opt-out of marketing, withdrawal processes for tracking data). The policy acknowledges users can opt-out of certain features without affecting other functions.
  - **Verdict**: Compliant. Users are given straightforward withdrawal mechanisms that respect prior consent for related processing.

### **Regulation Article 16: No Discrimination for Refusal of Consent**
Refusing consent must not lead to denial of services unless processing is required for the services themselves.

- **Privacy Policy Compliance**:
  The company does not deny service for refusing non-essential information (e.g., personalization, supplementary features). Refusal is allowed for device permissions without limiting core functions. However, mandatory real-name authentication is required for certain essential features (e.g., job application).
  - **Verdict**: Compliant. The policy specifies that non-essential data can be refused without service denial.

### **Regulation Article 17: Disclosure of Processing Information**
Processing information (processor identity, purpose, methods, types, duration) must be disclosed clearly and in an accessible format.

- **Privacy Policy Compliance**:
  The company provides detailed disclosures of processing purposes, methods, and types of collected information (e.g., account details, location data, sensitive information). Duration and storage mechanisms are described, with legal exceptions clearly stated.

  - **Verdict**: Compliant. The disclosure meets the requirements of clarity, completeness, and accessibility.

### **Analysis Outcome**:
The company appears to be largely compliant with the provided PIPL regulations. Its privacy policy demonstrates adherence to informed consent, lawful grounds for processing, clear mechanisms for withdrawal, and non-discrimination on refusal of consent. However, **areas needing vigilance** include:

1. **Lawful basis for Article 13 exceptions**: While the policy mentions legal mandates for certain types of processing, explicit justification for exception categories (e.g., public interests or statutory obligations) needs sharper alignment with Article 13 requirements.

2. **Implementation practices**: The policy promises compliance, but its practical implementation must align with the regulations, particularly in handling consent changes and ensuring transparency.

3. **Real-time updates**: If the company modifies services or sharing practices (e.g., third-party data sharing), explicit user re-consent is critical to comply with Article 17's notification requirements.

If discrepancies are found between policy promises and implementation, the company could face penalties under the PIPL for violations such as unauthorized data processing or inadequate consent management.